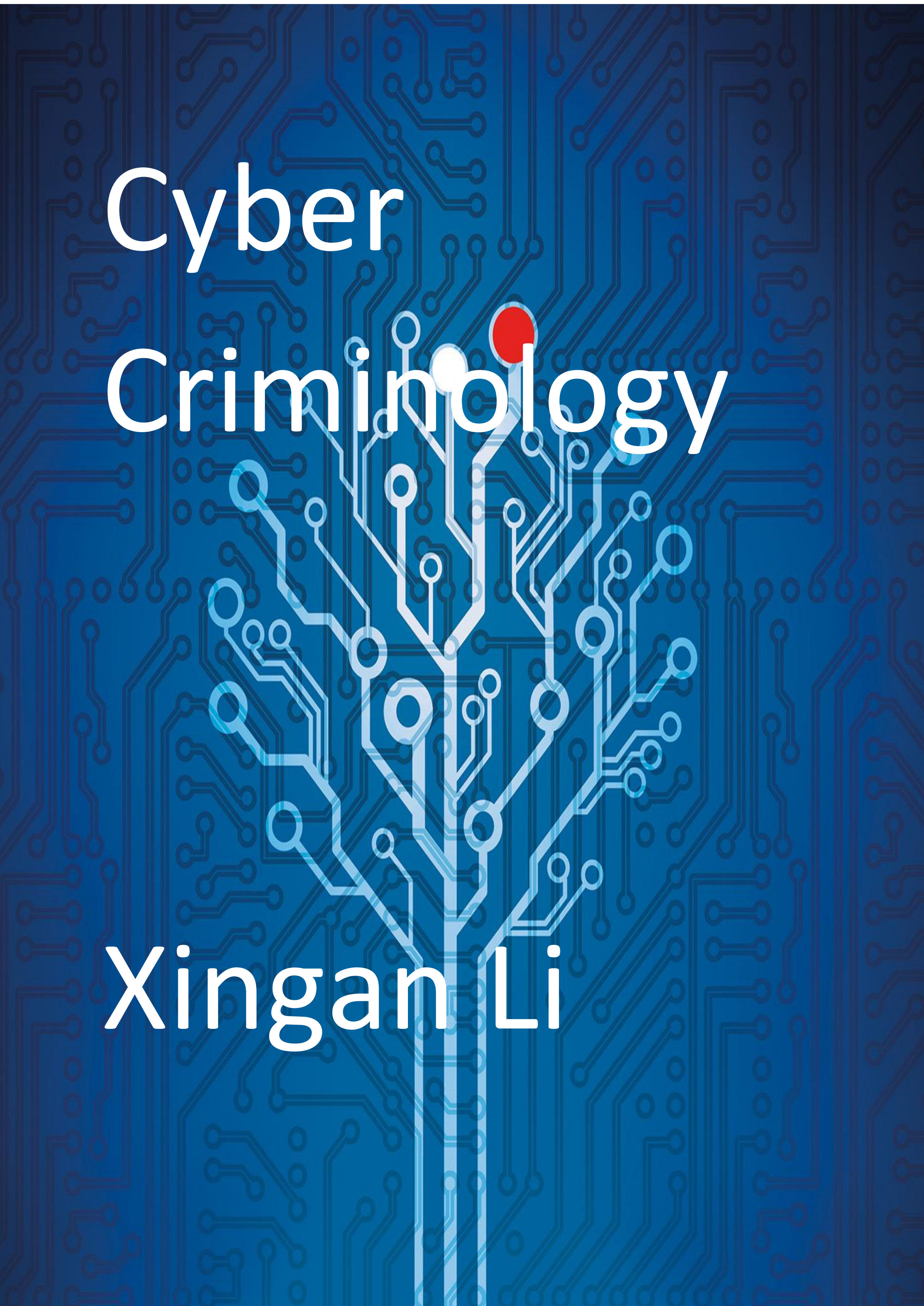


Cyber Criminology

Xingan Li

CYBER CRIMINOLOGY

Xingan Li
LLB, LLM, LLD, PhD
Associate Professor
School of Governance, Law and Society
Tallinn University, Estonia

TORONTO ACADEME PRESS

Made in Canada

Title: Cyber Criminology
First Edition, March 2017

ISBN 9780973981339 (PDF)

Publisher:
Toronto Academe Press
670 University Ave.
Charlottetown PE
C1E 1E3

Toronto Academe Press

Xingan Li

CYBER CRIMINOLOGY

Xingan Li

CYBER CRIMINOLOGY

PREFACE

Technological innovation, globalization, and urbanization have facilitated criminals and terrorists to pose a fresh wave of hazards that can shake the security establishment of global markets. The development of information and communications technology (ICT) creates not only advantages, convenience and efficiency, but also disadvantages, challenges and threats. Legislation is typically neither prompt nor sufficient enough to deal with technology-oriented social problems. The potential abuse of information systems has long been uncontrollable, and cybercrime has a deeply negative influence on the development of an information society. The risks of cybercrime have grown in recent years caused by technological advances, the growth in potential gains from committing cybercrime, and the lower probability of detection and punishment.

The book explores the conceived challenges created by the development of an information technology confronting the traditional social-control system. It proposes a definition in a broad sense, in which it identifies characteristics of cybercrime and their negative influence on the probability of detection and effectiveness of deterrence. Current legal frameworks on cybercrime, are found ineffective in combating cybercrime. The key understanding of this book is that,

in order for the information society to be protected and the effectiveness of legal deterrence to be guaranteed, it is imperative to eliminate legal and jurisdictional gaps between countries, and between meat space and cyberspace so as to hold the criminal subjects liable.

This book is an updated excerpt of my doctoral dissertation published in 2008, designed to provide readers with a phenomenological description of cybercrime. Readers will find it useful to have this new publication theoretically particular, interesting and useful. It can also be used as a textbook for courses on or a reference for research in cybercrime.

Xingan Li

Helsinki, Finland, March 2017

前言

技术革新、全球化和城市化使得犯罪分子和恐怖分子能够带来撼动全球市场安全的新威胁。信息通讯技术的发展不仅创造了优势、便利和效率，也带来了劣势、挑战和威胁。立法从来不能及时有效地对付因技术而生的社会问题。长期以来，对于信息系统的潜在的滥用难以控制，而网络犯罪对于信息社会的发展产生了深刻的负面影响。近些年来，由于技术的进步、潜在犯罪收益增长，以及侦查和惩罚概率低迷，网络犯罪的危险日渐增加。

本书探讨了信息技术发展对于传统社会控制机制树立的挑战。书中提出一个广义的定义方法，认定了网络犯罪的特点及其对于侦查概率和威慑效果的负面影响。可以发现，现行有关网络犯罪的法律框架在打击网络犯罪中其效甚微。本书的关键在于，为使信息社会得到保护，法律威慑取得实效，国家之间、传统空间与网络空间之间的法律与管辖的鸿沟必须去除，才能追究犯罪主体的刑事责任。

本书为笔者2008年出版的博士论文的摘编更新版，为读者提供一份网络犯罪的现象学论述。读者会发现本书在理论上具有独创性、趣味性和实用性。本书可以作为有关网络犯罪高级课程的教科书或者相关研究的参考书。

本书第一章导论部分介绍了网络安全和网络犯罪的社会背景。第二章和第三章聚焦于网络犯罪的现象学和类型学。本书提出一个统一

的广义定义，以便取得高度的国际共识。此外，作为对以前分类方法的发展，第三章根据信息系统在犯罪中的作用把网络犯罪分为七种类型，分别是信息系统被用作媒体、目标、工具、路径、地点、手段的犯罪和信息系统用于准备其他犯罪的网络犯罪。

第四章归纳网络犯罪人的特点和动机。随着网络用户和信息关联活动的增长，潜在的网络犯罪人获得更多的机会，出于不同的动机，发动不同规模的攻击。本章认定二十多种动机类型。传统犯罪向网络空间迁徙的可能性已经警示执法当局既打击现存网络犯罪，也积极预备应对新兴的威胁。

第五章分析网络犯罪的主要特征，特别是参考对其侦查与威慑的难度。本章主要考察犯罪行为人的特点、主观的情形、典型的被害人、时间与空间、技术的牵涉、复杂性、成本与损失、侦破与调查、管辖权的冲突以及网络犯罪现象的猖獗性。

第六章回顾网络犯罪与法律对策的历史发展。本章将发展过程分为四个阶段，表明网络犯罪现象几乎与信息通讯系统的发展同步进行。网络犯罪处于加速发展阶段，正在逐渐常规化，并且电子分裂导致网络犯罪分裂。基本结论是犯罪资源决定犯罪数量，而司法资源决定威慑。当犯罪资源与司法资源在长期过程中达成平衡时，犯罪现象将在一个平衡点达到饱和。

第七章研究网络犯罪责任的不同形式。犯罪的制裁具有必要性，但是现在与未来都不充分。民事救济可以补充刑事制裁。本章分析基于不同主体、法律基础、行为人的心理状态的责任、诸种责任的功能等。本章认为广泛覆盖的责任机制为打击犯罪所必需。

第八章聚焦于网络犯罪管辖权的主题。由于网络犯罪人的广泛分布和司法共识的缺乏，网络管辖权成为立法与司法必须解决的问题。有

必要创设行之有效的规则，连接地区、国家与国际边界。本章审视刑事管辖权的传统基础与重建刑事管辖权的若干新兴理论。本章提出基于责任的管辖权观点与网络犯罪管辖权的若干焦点。

第九章审视打击网络犯罪的国际刑法倡议。本章将国际协调行动分为专业的、地区的、多国的与全球的行动，概述了这些行动的主要关注，评估了《网络犯罪公约》在国内与国际法律层面的影响。本章也指出以往行动的局限性，预期联合国发挥更重要的作用。

最后，第十章归纳全书，强调网络犯罪与传统犯罪的区别，因此对法律体系提出挑战，而刑法在打击网络犯罪中起着必备的然而有限的作用。随着网络犯罪现象的常规化，刑法改革会随之减缓。总体上，应从脆弱性与动机的影响中找到解决方案。脆弱性应以技术手段消除，而动机则应以法律工具消除。

李兴安

芬兰赫尔辛基，2017 年 3 月

Table of Contents

LIST OF FIGURES

LIST OF TABLES

TABLE OF CASES

Alan Joseph Ogilvie v. Her Majesty's Advocate [2001] ScotHC 69 (27th July, 2001)

Allison, R. v. [1998] EWHC Admin 536 (13 May 1998).

Bohning v Government of the United States of America [2005] EWHC 2613

Boutrab, R. v. [2005] NICC 36 (24 November 2005)

Brown, R. v. 2006 CanLII 12302 (ON S.C.), Docket: C44863

Burns, R. v. [2003] NICC 13(2) (12 September 2003)

Debnath, R. v. [2005] EWCA Crim 3472, No. 200501008A7

DO, R. v. [2006] NICA 7 (10 March 2006)

Dooley, R. v. [2005] EWCA Crim 3093 (1 November 2005)

DPP v. Bignall [1997] EWHC Admin 476 (16 May 1997)

DPP v. Lennon [2006] EWHC 1201 (Admin) (11 May 2006)

Earthlink Inc. v. FCC (District of Columbia Circuit No. 05-1087, 15 August 2006)

Edward Yearly v. Crown Prosecution Service [1997] EWHC Admin 308 (21 March 1997)

Farkas, R. v. (2006 ONCJ 121, 10 April 2006)

Feltis, R. v. [1996] EWCA Crim 776 (19 August 1996).

Fischer v. Mt. Olive Lutheran Church (Western District of Wisconsin No. 01-C-0158-C, 28 March 2002)

Geller, R. v. 2003 CanLII 31190 (ON S.C.), Docket: 493

Godfrey v. Demon Internet Limited [1999] EWHC QB 244 (26th March, 1999)

Hamilton, R. v. 2005 SCC 47 (CanLII), Docket: 30021

Harlos, R. v., 2005 ABPC 118

I-SHO 13.11.2006 1401

Johnson, R. (on the application of) v. DPP [2005] EWHC 3123 (Admin) (8 December 2005)

Johnstone, R. v. [2003] UKHL 28 (22 May 2003)

Jones and Singh, R. v. [1997] EWCA Crim 164 (23 January 1997)

Kasam, R. v. 2004 ONCJ 136 (CanLII), Docket: 10018867

Kehoe & Anor, R. v. [1998] EWCA Crim 1163 (1 April 1998)

Kirkwood, R. v. [2005] EWCA Crim 3534 (21 December 2005)

KKO:1988:103 (Supreme Court Precedent of Finland)

KKO:1999:115 (Supreme Court Precedent of Finland)

KKO:2000:17 (Supreme Court Precedent of Finland)

KKO:2005:3 (Supreme Court Precedent of Finland)

KouHO:2005:11 (Court of Appeal Finland (Kouvola) Decision)

Kozun, R. v., 2007 MBPC 7

Kwok, R. v. 2007 CanLII 2942 (ON S.C.), Docket: P134/06

Lefave, R. v., Ontorio Supreme Court of Justice Court File No. CrimJ(P)6527/02 (3 October 2003)

Lloyd, R. v. [1996] EWCA Crim 1744 (17 December 1996)

McKinnon v. USA & Anor [2007] EWHC 762 (Admin) (03 April 2007)

Morgans v. Director of Public Prosecutions [2000] UKHL 9; [2000] 2 All ER 522; [2000] 2 WLR 386; [2000] Crim LR 576 (17th February, 2000)

Moseley, R. v. [1999] EWCA Crim 1089 (21 April 1999).

Novus Credit Services Inc v. Discover Financial Services LL C [2006] DRS 03205 (27 January 2006)

O'Brien, R. v., 2002 YKTC 94, Docket: 02-00176A • 02-00305

People of New York v. World Interactive Gaming Corp., 185 Misc. 2d 852, 714 N.Y.S.2d 844 (N.Y. County Sup. Ct. 1999).

Poon and Wong, R. v. 2006 BCSC 1824, Docket: 23635

Rees, R. v. [2000] EWCA Crim 55 (20 October 2000).

Reynolds & Ors, R. v [2007] EWCA Crim 538 (08 March 2007)

Robertson v. Her Majesty's Advocate [2004] ScotHC 11 (17 February 2004)

Robertson v. Newquest (Sunday Herald) Ltd & Ors [2006] ScotCS CSOH_97

RovHO 12.06.2001 335 (Court of Appeal Finland (Rovaniemi) Decision)

Royal Bank of Scotland Group PLC v. Laverio [2006] DRS 3953 (16 October 2006)

Russell, R. v. [2001] NICA 45 (12 October 2001)

State ex rel. McCleary v. Roberts (88 Ohio St.3d 365, 2000-Ohio-345

State v. Moning, 2002-Ohio-5097.

Taylor & Burin, R. v. [1997] EWCA Crim 1074 (2 May 1997)

Taylor, R. v. [1998] EWCA Crim 1545 (12th May, 1998)

Tektrol Limited v. International Insurance Company of Hanover Limited and Great Lakes Reinsurance (UK) Limited [2004] EWHC 2473 (Comm), No. 2003 folio 940.

THO:2005:28 (Court of Appeal Finland (Turku) Decision)

THO:2006:6 (Court of Appeal Finland (Turku) Decision)

Treleaven, R. v., 2006 ABPC 99 (24 April 2006)

Turner v News Group Newspapers Ltd. & Anor [2005] EWHC 892 (QB) (12 May 2005)

United Sates v. Millot (Eighth Circuit No. 04-3962, 15 November 2005)

United Sates v. Pitts (Fourth Circuit No. 97-4616, 28 January 1999)

United Sates v. Steiger (Eleventh Circuit No. 01-15788, 01-16100 and 01-16269, 14 January 2003)

United State v. Lloyd (D. JN 26 February 2002)

United Stated v. Newson (Seventh Circuit No. 03-3366, 5 April 2004)

United States v. Angevine (Tenth Circuit No. 01-6097, D. C. No. 00-CR-106-M, 22 February 2002)

United States v. Cabrera (Eleventh Circuit Nos. 98-4432, 98-4434, D .C. Nos. 96-CR-562-DLG, 98-CR-77-DLG, 19 April 1999)

United States v. Carlson (Third Circuit No. 05-3562, 12 December 2006)

United States v. Christopher Lee Adjani; Jana Reinhold (No. 05-50092 D. C. No. CR-04-00199-TJH-01 OPINION, 13 January 2006)

United States v. Clayton (Ninth Circuit No. 96-10127, 11 March 1997)

United States v. Czubinski (First Circuit No. 96-1317, 21 February 1997)

United States v. Desir (Western District of Pennsylvanie 2005)

United States v. Diaz (S. D. Fla. 5 December 2003)

United States v. Garcia (C. D. Cal. 23 February 2004)

United States v. Gorshkov (W.D. Wash 4 October 2002)

United States v. Ivanov (D. Conn. 25 July 2003)

United States v. Jarrett (Fourth Circuit No. 02-4953, 3 June, 2003)

United States v. Long (the Seventh Circuit No. 04-1721, 22 February, 2005)

United States v. Magnuson (Fourth Circuit No. 964957, D. C. No. CR-96-186-A, 24 June 1997)

United States v. McKenna (D. NH 18 June 2001)

United States v. McKinnon I (E.D. Va.) and II (D. N.J. 12 November 2002)

United States v. Meek (No. 03-10042, 12 January 2004)

United States v. Middleton (Ninth Circuit No. 99-10518, 12 September 2000)

United States v. Muick (Seventh Circuit No. 97-CR-30004, 8 February 1999)

United States v. Patterson (W. D. Pa. 2 December 2003)

United States v. Pierre-Louis (Southern District of Florida No. 00-434-CR-GOLD/SIMONTON, 22 March 2002)

United States v. Ray (Eighth Circuit, No. 05-1655, 15 November 2005)

United States v. Ropp (C. D. California, 7 October 2004)

United States v. Sablan (Ninth Circuit No. 94-10533, D. C. No. CR-94-00017-JSU, 7 August 1996)

United States v. Slanina (First Circuit, No. 00-20926, 12 February 2002)

United States v. Sullivan (Fourth Circuit No. 01-4330, 25 January 2002)

United States v. Sullivan (W. D. NC, 13 April 2001)

United States v. Tenebaum (18 March 1998)

United States v. Thomas (1996 FED App. 0032P (Sixth Circuit)

United States v. Upham (First Circuit No. 98-1121, 12 February 1999)

United States v. Ventimiglia (M. D. FL 20 March 2001)

United States v. Zezev (S.D. N.Y. 1 July 2003)

United States v. Ziegler (No. 05-30177 D. C. No. CR-03-00008-RFC ORDER AND OPINION, 6 March 2007)

Wood, R. v. [1982] 767 Cr. App. Rep. 23.

X v. European Central Bank. (Officials) [2001] EUECJ T-333/99 (18 October 2001)

Yearly v. Crown Prosecution Service [1997] EWHC Admin 308 (21st March, 1997)

ABBREVIATIONS

APEC Asia-Pacific Economic Cooperation

ATM Automatic Teller Machine

BBS Bulletin-board System

CCIPS Computer Crime and Intellectual Property Section

CERT Computer Emergency Response Team

CoE Council of Europe

CSI Computer Security Institute

CSIS Centre for Strategic and International Studies

EU The European Union

FBI Federal Bureau of Investigation

ICT Information and Communications Technology

Interpol International Criminal Police Organization

IP Internet Protocol

ISP Internet Service Provider

ITU International Telecommunication Union

KKO Korkein oikeus (The Supreme Court of Finland)

KouHo Kouvolan hovioikeus (Court of Appeal Finland (Kouvola))

LAN Local Area Network

MIT Massachusetts Institute of Technology

NII National Information Infrastructure

NIPC National Infrastructure Protection Centre

NIST National Institute of Standards and Technology

OAS Organization of American States

OECD Organization for Economic Cooperation and Development

PUMA Public Management Service

REMJA Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas

RovHO Rovaniemen hovioikeus (Court of Appeal Finland (Rovaniemi))

SNSs Social Networking Services

THO Turun hovioikeus (Court of Appeal Finland (Turku))

U. K. The United Kingdom

U. S. The United States

UN The United Nations

UNCJIN United Nations Crime and Justice Information Network

WSIS World Summit on the Information Society

WWW World Wide Web

CHAPTER 1 INTRODUCTION

1.1 Social context of cybersecurity and cybercrime

Recent decades have witnessed a golden age in social history, previously symbolized by long wars and disasters, but now showing a scene of unparalleled development in information and communications technology (ICT) and related material forms of computers and networks. In both academic and popular discourses, newly-coined words indicate that the information age has arrived and an information society has emerged. The emancipation of the Internet from monopolistic control to open access to the public at the end of the twentieth century brought about a revolutionary epoch for human beings (Adamson, p. 37). The transition eliminated primary obstacles to information accessibility. That ICT reshapes business, the economy, education, entertainment, the media, the military, politics, as well as other social institutions in remarkable ways has already become a well-established common viewpoint. Few in international societies deny the fact that ICT is beneficial to states, organizations and individuals: it is an influential tool of development for the economies, a mechanism offering opportunities to overcome various traditional obstacles to development; and a medium increasing individuals'

active participation in social affairs and improving their competence in markets.[1] Reality sufficiently justifies the discourse: in 2007, the global networks of information systems have connected approximately 1.15 billion people (Internetworldstats.com 2007), while in 2015, the number is nearly tripled and reached 3.27 billion (Internetworldstats.com 2015). In 2007, more than one-fourth of them are online Europeans, who have the penetration rate of 39.8 percent (Ibid). In the European Union alone, the 255.58 million Internet users represent an average of more than half the whole population in these countries (Internetworldstats.com 2007). Today, users in Asia constitute nearly half of world Internet population (Internetworldstats.com 2015). The number of European users falls into not more than one fifth (Ibid.). The overall number of world Internet users increased eightfold (Ibid).

As one of the fast increasing fields, Social Networking Services (SNSs) spread in a surprising rhythm into contemporary social life. While the number of users of the SNSs is not available, it was estimated that among Internet users, about 74% of online adults use social networking sites (Pew Research Center 2015). In fact, at present, SNSs are used in a broad range of mobile devices, such as smart phones, cameras, media players, tablets and phablets, and notebook PCs, which are usually connected to the networks when they are in use.

Information systems are designed to serve people.[2] Application of the Internet has created a focus of attention for an increasing number of

[1] The Commonwealth, Malta Declaration on Networking the Commonwealth for Development, Commonwealth Heads of Government Meeting (CHOGM), 25-27 November 2005.

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October

individuals, organizations and governmental agencies. The networks connect a formerly offline population into an online cyberspace,[3] which is relatively separated from and independent of traditional society. It is considered as a virtual environment where netizens[4] live a virtual life, communicating with e-mail, chat rooms, instant messenger, and the bulletin-board system. They engage in teleworking;[5] going e-shopping; and are educated partially by means of computer-assisted learning,[6] taking part in net-based courses; and carrying out e-commerce through electronic marketing.[7] It is often anticipated that e-

---

1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, Preamble (2).

[3] Cyberspace is a term coined by William Gibson in Neuromancer (Gibson, 1984). An a popular definition of cyberspace, it includes all of the computers and other digital devices that are connected to both internal and external networks and can communicate with each other (Sadowsky and co-workers 2003, p. 16). In recent years, the prefix "cyber-" has been widely used in both academic works and governmental documents. The original meaning of "cyber" means computer (Pickett and co-workers, 2000). However, this prefix was not broadly used before computer networks became common. In fact, the origin of the prefix "cyber" has been traced back to human-machine interconnection (Jones 2003, p. 112). Therefore, the public understanding of this prefix relates to the meaning of computer networks, particularly the Internet. In this book, I also use this prefix in terms of computer and computer networks, but the emphasis is put on the whole information system rather than simply on the hardware.

[4] Netizen is a term used to indicate citizen in the Internet community, the counterpart of which is a citizen in the traditional community.

[5] According to Daintith (2004, p. 529), when computers and telecommunications are used in remote working, usually outside office, the activity is called teleworking. For detailed discussion and prospects on the teleworking environment, Shoni, Jackson, Hollmen and Aspnäs (eds., 1998).

[6] Computer-based learning is usually termed as e-learning, or CBT (computer-based training) (Rosenberg, 2001).

[7] Commerce has been developing from traditional commerce through c-commerce (computerised commerce (Royall and Hughes 1990, p. 8), e-commerce to m-commerce. E-commerce is the abbreviated form of electronic commerce, referring to commerce using electronic media, usually, the Internet (Daintith 2004, p. 173). At present, when people say e-commerce, the general meaning of this term is commerce through the Internet. As far as commerce through the mobile network is concerned, people utilize the term m-commerce.

government will govern them by means such as e-governance.[8] This virtual society is, however, still in the imagination or expectation, and society is far from splitting into a traditional society and a cyber society. However, at the same time, we cannot simply ignore the great influence of projects such as "Europe's Information Society."[9] To extend Coleman's social theory (1990), it can be said that there are signs of a cyber physical environment and of a cyber social environment, which is being constructed on information systems and by netizens armed with information.

Unfortunately, information systems are likely to crash, and likely to cause disputes and lawsuits.[10] Furthermore, the order of cyberspace, closely associated with the welfare of citizens, the security of businesses, and the stability of society is, however, becoming increasingly significant, due to increased scale of the online population to over one-sixth of the inhabitants of the globe (for an exploration of social order in cyberspace, see Li 2014b, 2015). What is problematic in the landscape of the social sciences is that many technological loopholes are constantly being exploited with malicious intent,

---

[8] According to Bharnagar (2004, p. 21), "the term e-government is sometimes confused with e-governance and the two terms are often used interchangeably. E-governance has been defined as the process of enabling transactions between concerned groups and the government through multiple channels by linking all transaction points, decision points, enforcing/implementation points and repositories of data using information and communication technologies, to improve the efficiency, transparency, accountability and effectiveness of a government."

[9] European Commission, Europe's Information Society-Thematic Portal. Retrieved 15 February 2016, from http://ec.europa.eu/information_society/index_en.htm

[10] In KKO:1988:103, a lawsuit was brought about on employee's holiday compensation miscalculated due to the fault of the computer programme. In KKO:2005:3, the issue in dispute was that the advocate of a convicted person had sent an appeal against the conviction through an e-mail message and within the time limit, but the advocate received an answer in the form of an e-mail message from the court, stating that no e-mail massage had ever arrived and so no appeal had been received against the conviction within the time limit.

while technological opportunities are, at the same time, generating various benefits as well. Hence chaos, disorder, social problems, and more severely, crimes pose great threats to the security, reliability, and credibility of the information society.

Cybersecurity has extended its influence into "meat space", that is, real society, and caused widespread concerns among various entities (Li 2006a). It has long been recognized as one of the issues deserving consideration in normal social life (for example, Aromaa and Laitinen 1994, pp. 47-101). As a typical example, the American Computer Science and Telecommunications Board of National Research Council (2002, pp. 1-2) has stated that, cybersecurity has always been the central concern in a series of their research studies in the past decade. It is also true for many other institutions, which invest considerable human resources and financial resources in their work.[11] Cybercrimes,[12] criminal offences committed by netizens in cyberspace, are new variants of criminal phenomena. This raises many questions as to whether the existing legal system has the capability of deterring cybercrimes.

The development of crime is closely related to social transformation at both the micro and the macro levels. Two factors symbolize the severity of this criminality: On the one hand, it is growing at a rapid speed; on the other hand, it is a serious problem for both private and public sectors (Bequai 1983, p. 3). For the public, everyone faces the threat with same acceleration. With the

---

11 It is neither necessary nor possible to give an academically exhaustive list of these institutions. But I would like to empirically name a few: the UN, the EU, the CoE, the OAS, the APEC, the ASEAN, the OECD, the FBI, the ITU, etc.

12 Perrin (2005) stated that the term cybercrime was coined in the late 1990s when the G8's Lyon Group used the term to describe criminal phenomena existing in the information and communications networks.

emergence, development, and rampancy of cybercrime, cybercriminology, a new discipline, is acquiring an independent position. The studies of cybercriminal phenomena, its causes and motivations, and models for the prevention of cybercrime, compose the essential outline of cybercriminology.

Traditionally, criminology has been composed of a variety of parallel theories in explaining criminal phenomena in general and as well as in specific offences. Causal factors and deterrence have constantly been the focuses of many different schools in this field.

Cohen and Felson's routine-activity theory (1979) provides a trichotomized method in reducing causal factors of crime to presence of motivated offenders and potential victims, and to the absence of effective guardianship. Broad attention has been paid to the theory in the last two decades. Grabosky and co-workers (2000) have applied the routine-activity theory to explain the causes of certain theft offences in cyberspace, stating that cybercrime might be explained by the combination of three factors: motivation, opportunity and the absence of capable guardianship, just like crime in general (See also Grabosky 2000, p. 1). This book continues the analysis that Grabosky and co-workers have started, and seeks to incorporate the three factors in Cohen and Felson's theoretical structure (1979) into social disorganization theory.

Social change has both physical and psychological consequences for society and people, as well as for control mechanisms. Thus social change theory can well be installed at the sublevel of the routine-activity theory to reinforce the latter's explaining power during rapid social transformation.

Another theory is the social disorganization theory initiated by Thomas

and Znaniecki (1927) and developed by Cooley (1983). The disorganization of society has broad physical and psychological impacts. At the same time, it means the disintegration of the existing social-control mechanisms.

In Li (2008b), social change theory was incoporated into the social disorganization theory. The reason for such an effort is that the prevalence of information and communications technology and the proliferation of information itself signifies a great social transformation from members of society being weakly informed to members of society being more strongly informed. During this process, the old setting of previous social structure and relations that facilitated information access has been reshaped into a new set of social structures and relations. In the sense that the old order was dissolved while the new order has not fully established, there emerges a period during which a new process of social disorganization is occurring.

Social change not only directly leads to the presence of potential offenders and victims, as well as to the ineffectiveness of guardianship, but also leads to social disorganization. Furthermore, social disorganization not only happens as a result of social change, but also happens because of other factors. Whatever the reasons by which social disorganization emerges, it will lead to the triplet factors (motivated offenders, exposure of victims, and absence of guardianship) that influence the occurrence of crime.

Cybercrime is usually regarded as a legal phenomenon regulated through criminal law, which is a branch of law that has the longest history, dealing as it does, with issues of crime and punishment. Feldman (1993, pp. 4-6) claimed that criminal law has a moving border accommodating crimes of various forms, implying that offences may be criminalized or decriminalized over time or

across jurisdictions. In the temporal dimension, the change of criminal law over time necessitates legal reform, while in the spatial dimension, the difference in criminal laws between the various countries requires international harmonization. The emergence of cybercrime engenders both challenges. Analysing the elements of cybercrime helps to structure the legal system in the new field. The process of criminalization and penalization of various cybercrimes must be based on the reorganization and reconstruction of traditional criminal law. The incorporation of cybercrime not only increases the quantity of clauses, but also enriches the content of criminal law; it not only influences the literal provisions, but also helps to update the conventional notions; not only does it take into account the criminal "law," but it also considers criminal policy. The general principle of criminal law has been concluded as "nullum crimen, nulla poena sine lege."[13] Nevertheless, at the

---

[13] The Latin maxim literally means that "no crime, no penalty without law." Initially incorporated by Paul Johann Anselm Ritter von Feuerbach as part of the Bavarian Code in 1813, the principle has been broadly adopted in both national and international laws. Many countries provide for the principle in their constitutions. For example, Chapter 1 Section 8 of Constitution of Finland provides the principle of legality in criminal cases, saying that "No one shall be found guilty of a criminal offence or be sentenced to a punishment on the basis of a deed, which has not been determined punishable by an Act at the time of its commission. The penalty imposed for an offence shall not be more severe than that provided by an Act at the time of commission of the offence." (Constitution (731/1999), Translation provided by Finland Ministry of Justice).

Other countries provide it in their criminal laws. For example, Section 1 of Criminal Code of Germany provides that "An act may only be punished if its punishability was determined by law before the act was committed." (As promulgated on 13 November 1998. Translation provided by the Germany Federal Ministry of Justice) International agreements also adopted this principle. For example, Article 22 of Rome Statute of the International Criminal Court, 17 July 1998 prescribes that "1. A person shall not be criminally responsible under this Statute unless the conduct in question constitutes, at the time it takes place, a crime within the jurisdiction of the Court. 2. The definition of a crime shall be strictly construed and shall not be extended by analogy. In case of ambiguity, the definition shall be interpreted in favour of the person being investigated,

same time, "[E]ven those laws which have been written down are best regarded as not unchangeable." (Aristotle Aristotle, cited in Vernant, Jean-Pierre ed., 1995, p. 148) Timely amendment is a prerequisite for a penal code to meet the need of social change and for combating crimes.

As a social phenomenon, crimes change with the development of society. It has previously been recognized that with the advent of ICT, social change brought about by technology is capable of occurring with devastating rapidity. Social scientists should make efforts to identify the bases of the transformation occurring in the information age, a transformation which is happening faster than ever before (Peters 1971, p. 31). The theme considered within this book is that despite the fact that society is increasingly dependent on information systems, cybercrime is eroding the underpinning of this society. "How to implement appropriate sanctions on cybercrime?" becomes one of the important questions society ought to answer. There have already been a number of preliminary efforts to analyse cybercrime and punishment, though the current achievement are somewhat fragmentary.

While ICT is an instrument that people designate to promote social welfare, the distinctive nature of cybercrime is social harm. The technology itself, nevertheless, contains no value judgment. It can only be used to satisfy revelation of both virtue and vice. Even if people deliberately use the technology to promote virtue and to restrain vice, this can have only a limited function. The purpose of all laws, particularly criminal law, is to protect individual, collective, public, or state interests by using the threat of punishment

---

prosecuted or convicted… " Article 7 (1) of European Convention on Human Right has a similar provision.

and by executing punishment to make the threat realized. But with cyber offences something more is needed. Consequently, the liability mechanism has been deployed as a necessary remedy for the abuse and misuse of technology.

At the same time, the vulnerability of information systems[14] exposes them to potential threats from social actors motivated by different desires. As Bertrand Russell stated that, "Life is nothing but a competition to be the criminal rather than the victim" (Russell 1920, in Griffin 2001, p. 215). Due to the potential for harm, cybercrimes and cybercriminals certainly concern governments, law enforcement, and international organizations. The liability of cybercrime has become a new subject-matter in criminal law, tort law, and even contract law.

As Smith, Grabosky and Urbas (2004) pointed out that, (their) previous studies had carefully described likely kinds of digital crimes and had furnished many appropriate preventive measures to stop crimes of this nature (p. 14). In order for our society to continue to flourish, legal certainty should be extended to guarantee that criminal activities committed in cyberspace are punished in the physical world. Starting from the accepted premise that social science theory can add help design and shape the social process (Coleman 1990), this book focuses on the criminalization of offences, the harmonization of jurisdiction, international cooperation, and integrative prevention mechanisms.

[14] According to the U. S. Federal Standard 1037 C, the term information system has the following meanings: "1. A system, whether automated or manual, that comprises people, machines, and/or methods organised to collect, process, transmit, and disseminate data that represent user information. 2. Any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware." See Federal Standard 1037C, MIL-STD-188.

It will review and evaluate critical factors confronting the criminal-law system so as to give feasible policy recommendations for dealing with cybercrimes more effectively.

1.2 Structure of this book

After this Introduction, to address the challenges posed to criminal law by information systems, it is necessary to clarify how the phenomenon stands from the legal viewpoint. Chapter 2 and Chapter 3 concentrate on the phenomenology and typology of cybercrime. The book proposes a unified definition in a broad sense in order to reach a high degree of international consensus. In addition, as a development of a previous classification method, Chapter 3 divides cybercrimes into seven categories according to the different roles that information systems play: crime in which information systems are used as media, target, tool, route, place, means, and crime in which information systems are used in preparation for further offences.

Chapter 4 looks at the characteristics and motives of cybercriminals. With the increase of Internet users and information-related activities, the potential cybercriminals acquire more opportunities to launch attacks of different scales and from different motives. This chapter identifies more than twenty types of motive. The possibility of moving traditional crimes into cyberspace has alerted law enforcement to fight against existing cybercrime and to prepare for emerging threats.

Chapter 5 analyses the primary characteristics of cybercrime with special reference to its detection and deterrence. The characteristics of the perpetrators,

the subjective situation, the typical victims, time and space, technological involvement, complexity, costs and losses, detection and investigation, conflicts of jurisdiction, and rampancy of the cybercriminal phenomenon will be examined.

In Chapter 6, the book reviews the historical development of cybercrime and legal countermeasures. The chapter divides the process into four stages and concludes that cybercriminal phenomena have developed almost synchronously with ICT. Cybercrimes are in a process of accelerating development and are becoming gradually routinized. While the electronic divide thus results in cybercrime divide. The basic conclusion is that criminal resources decide the amount of crime, while judicial resources decide the deterrence. When the balance is reached between criminal resources and judicial resources in the long term, the criminal phenomena will be saturated at an equilibrium point.

Chapter 7 studies the various forms of liabilities of cybercrime. Criminal sanctions are necessary but are currently neither in being nor will be sufficient alone. Civil remedies can be complementary to the criminal sanctions. The chapter also analyses liabilities based on different subjects, legal bases, the psychological status of the perpetrator, functions of the liabilities, and so on. The chapter concludes that a liability mechanism of broad coverage is necessary to combat cybercrime.

Chapter 8 focuses on the theme of cybercriminal jurisdiction. Because of wide distribution of cybercriminals and the lack of legal consensus, cyberjurisdiction is becoming a problem that legislation and law enforcement must deal with. It is necessary to create workable rules that bridge the local, national, and international boundaries. This chapter reviews the traditional basis

of criminal jurisdiction and some new theories concerning the rebuilding of a basis for criminal jurisdiction. The chapter concludes with the idea of a liability-based jurisdiction and some focal points of cybercriminal jurisdiction.

Chapter 9 reviews the international impetus of criminal-law initiatives in combating cybercrime. This chapter classifies the actions of international harmonization into professional, regional, multinational and global actions, summarizes the major concerns arising from these actions, and evaluates the influence of the Convention on Cybercrime at the national and international levels of legal countermeasures. The chapter also points out the limitations of the previous actions and anticipates the UN playing a more important role.

Finally, Chapter 10 concludes the whole book by emphasizing that cybercrimes are different from traditional crimes and thus pose new challenges to the legal systems, and that criminal law plays a necessary but limited role in combating cybercrime. With the routinization of the phenomenon of cybercrime, criminal-law reform will slow down. Overall, solutions should be found from the impacts of vulnerabilities and motives. The vulnerabilities should be eliminated by technological means, while the motives should be eliminated by legal instruments.

CHAPTER 2 DECIPHERING THE PHENOMENON OF CYBERCRIME

2.1 Introduction

Although the pervasive use of information systems is accompanied by a wide range of social problems, and the countermeasures necessitate mobilizing a broad variety of legal remedies, the current book will primarily be concentrating on the criminal phenomenon accompanying information systems and on the deterrence framework revolving around but not limited to criminal law. Therefore, the main task facing us is to determine the scope of the topic, through defining the subject-matter "cybercrime".

Alternative definitions of cybercrime have emerged over the years as the users and abusers of computers expand into new areas. There is neither a unified definition, nor a commonly accepted method of classification. The definition and classification methods are so diversified that it is impossible to sketch the scenario of cybercrime by using a single standard (Wasik 1991, p. 1). The present rampancy of cybercrime can in part be understood as the product of weak legal deterrence. This chapter advocates the use of a unified broad definition of cybercrime, in order to reach a consensus as great as possible,

reform both substantive and procedural criminal law and provide effective protection for the information society. The chapter also proposes to classify cybercrime according to the roles of information systems into seven categories, information systems as target, tool, media, route, place, means of crime, and used in preparation for further offences.

2.2 Development of definition of computer crime

Before the 1990s, computer crimes were generally understood as offences relating to computers, but there was less connection with networks, even though the perpetrators of earlier computer crimes also exploited the networks. Among scholars, the disputes concerning the relationship between computer and crime were diverse. Even today, there is no apparent distinction between a computer crime and a traditional crime that has some factors relating to the computer or the Internet. The situation in the pre-Internet age should easily be realized from the present viewpoint. However, the most noteworthy dispute then resolved around whether there was a distinct criminal phenomenon of computer crime. Roughly, three different standpoints existed.

From the first standpoint, there was no such thing as computer crime. For example, Johnson (1985) insisted that there was no distinction between an offence involving a computer and an offence involving no computer. Gotternbarn (1990, pp. 18-24) also claimed that a particular category of computer crime was unnecessary. The negativists regarded computer crimes as offences belonging to traditional categories. Because murder with a wooden

stick, a block of stone, a knife, a gun, or a bomb, was only a murder, naturally theft by with a bag, a car, or a computer remained just a theft. The "new" types of crimes or new forms of existing crimes could, from this standpoint, be covered by traditional criminal law. There was, therefore, no need to add new articles to existing law. The only task was to punish these crimes according to the old law.

The second standpoint claimed that the computer could be used to perpetrate every kind of crime. It could be considered pan-computer crime view (Nycum 1983, pp. 2-4). According to Sterling (1994), Donn B. Parker claimed that "…all business crime will be computer crime, because businesses will do everything through computers. 'Computer crime' as a category will vanish." Li (1993) proposed that computer crime was neither a single offence, nor a category of offences; only because the offences more or less related to computer systems, they were called computer crimes. In fact, this term refers to one kind of computer crime in one situation, and referred to one category in other situations. The computer crime thus covered a very broad range of offences.

Li (1992) also attempted to apply traditional penal law provisions to various possible kinds of computer crimes, in examining the possibility of using the 1979 Penal Law of China to impose a penalty on all offences involving computers against state security, person, property, and the social order. This kind of proposal was also a universally accepted idea about dealing with computer crime in many countries at that time. The evidence was that many countries punished the first computer crimes before they implemented their first computer crime laws. At least in countries where a broad legal

interpretation and judicial legislation were practised, unpunished computer crime cases due to lack of applicable law were rare. But the *analogous application of law* by extending the scope of existing law to impose punishment on activities that were not prescribed by law when they were committed is prohibited by the principle of legality. The *broad interpretation of law* did not necessarily, however, violate the principle of legality, even if the interpretation incorporated new terms such as the computer, the Internet, and information systems into law where these terms were once absent. The value of this standpoint was to make the potential of traditional criminal law as great as possible. Where there is no law ready to combat computer crime, this standpoint provides a theoretical basis for the application of existing laws to both protecting society and maintaining legality.

In practice, as Bequai (1978) wrote that, "the majority of our local jurisdictions rely on traditional concepts to deal with this new and growing area of crime" (p. 25), including laws dealing with crimes involving habitation and occupation, covering arson and burglary; and laws dealing with offences involving property, covering larceny, embezzlement, extortion, malicious mischief and forgery (pp. 25-36). Recent efforts for utilizing the functions of existing criminal law have also been made in Brenner (2001).

The third standpoint was held by middle-of-the-roaders, who admitted the existence of computer crime on the one hand, but limited the range of offences on the other. Undeniably, this has been the most broadly accepted theory. According to this theory, different technical terms have been used to denote the phenomenon, different definitions have been given to describe the issue, and different theoretical achievements have been acquired to address the legal

framework. However, it must clearly be recognized that there has never been a unified technical term, a unified definition (UNCJIN 1999, Paragraph 21), or a unified theoretical structure of a globally accepted kind. Many technical terms have been used interchangeably.[15] Different countries and individuals have referred to many definitions. In addition, people from different disciplines have also developed many theoretical frameworks over the years. At present, when we talk about computer crime, or cybercrime, a direct reflection of this is the assumption that computers or networks are involved in this crime.

Computer crime has been defined in a diverse spectrum of senses, from extremely narrow ones to extremely broad ones. The definition in the narrowest sense limits computer crime to "one that can be carried out only through the use of computer technology" (Tavani 2000, pp. 6-7). This definition excludes crimes that can be committed only through other means than computer technology and that can be committed in both ways. A broader approach defines computer crime as crime by computer. This definition excludes crimes targeting a computer.

A yet broader definition includes both crimes by computer and against the computer.[16] The current view about offences against computers is likely to relate the physical forms of computers or computer technology to the function of computers. There were numerous cases in which computers were damaged not by today's technological methods, such as viruses, hacking etc., but were committed by traditional measures, including arson, bombing, and shooting.

---

[15] See COM (2000) 890 final, 12. Even the UN uses the terms computer crime and computer-related crime interchangeably. See also United Nations Crime and Justice Information Network (1999), Paragraph 21.

[16] See, for example, McConnell International (2000); Reece (2000). See also Berg (2000); Goodman (1997), pp. 465, 468-469.

The development of cybercriminal phenomena proves that there is a vague limit between offences by computer and offences against the computer.

The broadest definition was proposed by Parker (1980, cited in Solarz 1981, pp. 25-26), who divided computer crimes into computer abuse, computer crime and computer-related crime. Obviously, the computer crime conception at the second level was included in the first level. The computer crime conception at the first level was extremely broad. In fact, Parker and Nycum (1984, p. 313) defined computer crime "as any illegal act where a specific knowledge of computer technology is essential for its perpetration, investigation, or prosecution," saying subsequently that computer crime was not regarded as a distinct type of crime different from other crimes, and that almost every sort of crime could be committed through the exploitation or intervention of computers (ibid). Such kind of a definition has accepted and developed by many subsequent studies, for example, Pihlajamäki (2004) defined cybercrime ("information technology crime" in his original term) as a crime in which the data processing system is the target or tool, while special knowledge of information technology is a necessary factor in the process of commission and prosecution (p. 286).

In the network environment, the model of a computer crime becomes more relevant with the emergence of the Internet. Cybercrime is loosely defined as a crime committed by means of the computer or the Internet (Levinson 2002, p. 455). The Council of Europe Convention on Cybercrime 2001 made the term "cybercrime" prevalent. Articles 2-10 of the Convention on Cybercrime also adopted a broad conception in criminalizing cybercrime, providing for the offences against security, computer-related offences, and

content-related offences. Although the Convention adopted a broad conception, the detailed offences under the titles were limited. The high level of consensus concerning conception, and the low level of consensus concerning the categories is a factor that makes it reluctant for more countries to consider access to the treaty.

2.3 Analysis of the previous shortcomings in defining cybercrime

Some of the previous understanding about cybercrime has been misleading and confusing in providing inexact information. The following deficiencies have been very frequent in both academic writings and non-academic writings.

The first misunderstanding happened against a historical background. While people have regarded the predecessors of cybercriminals as the hackers of three or four decades ago, a general view has been to make the term "hacking" bear the meanings of today's "cybercrime". This misunderstanding buried the computer explorers collectively under the shell of deviance.

The increasing cyber perpetration at the end of the twentieth century and the beginning of the twenty-first century witnessed a second misunderstanding of the conception. The illusion that information systems were a critical infrastructure that was easily prone to abuse and in effect caused massive deaths, injuries, and economic disasters led to an extreme notion that viewed all cybercrimes as terrorist attacks. The equation "cybercrime = cyber terrorism" has already been broadly accepted by many scholars with the help of a non-expertise dominated mass media, which survive competition by spreading both

truth and speciousness. As yet, although there have been many concerns about the use of information systems in the preparation of real terrorist attacks, and the situation may be growing worse,[17] cyber terrorism is only a political possibility. The crime is the premise of punishment that assumes a legal order, but the terrorism is a reason for war that destroys the legal order. By exaggerating many traditional crimes as terrorism, the powers can launch continues wars against the weaker states, or threaten to do so as politics. By claiming all cybercrime as cyber terrorism, the future of the communities in the information society is obscure. We doubt whether hackers deserve punishment by war. The character of such a war would not be its punitive nature, but a social collapse.

The third misunderstanding is politicization of the conception in a broader sense. To view cybercrime as cyber terrorism is one part of the picture. This broad misunderstanding was created by the acclamation of information systems as a national critical infrastructure, to maintain and protect which the state intervention or political intervention is considered necessary. The politicization of information systems results in the politicization of activities against this system, the cybercrime.

The fourth misleading understanding is, strangely, to moralize the cybercrime by exploiting the term "hacking". The moralization has two respects: one regards cybercrime as being moral, not immoral and thus not illegal; the

[17] Many prosecuted cases involved features that were possibly to be used in terrorist attacks deposited in information systems, for example, R. v. Boutrab ([2005] NICC 36 (24 November 2005)), in which the accused downloaded from a library computer and deposited in floppy discs the files, the contents of which contained information about the making and use of explosives for attacks on aircraft and the manufacture of silencers for firearms.

other regards cybercrime as a moral issue, not a legal issue, and thus law has no business here. The natural effect is that cybercrime should not be regulated by law.

The last category of misleading definitions has the tendency of mystification. The representative notion is that cybercrime is high-tech crime and does not seem to be committable by common users in daily life. Actually, when technology is used in routine life, high technology gradually becomes low technology. When high tech crime exists in daily life, it becomes low-tech crime.

2.4 How to define cybercrime?

No unified term for cybercriminal phenomena has been universally accepted, even though some terms including "computer crime" and "cybercrime" are relatively popular. Roughly, seven groups of terms have been in use. Among these groups, many different words and phrases have been adopted or created. Because of the changing ways in which the cybercriminals commit crimes, the ways in which people name these crimes are changing as well. In order to clarify how people view cybercrime from different standpoints, this section examines some groups of synonymous terminologies of "cybercrime".

The first group of terms emphasizes the view that regards the computer as a unique target or tool of crime. The term "computer crime" has been broadly used in academic writings as well as in laws and regulations particularly before the Internet was opened to commercial use in the 1990s. This term represents a

group of similar terms, including computer crime,[18] crime by computer (Parker 1976), computer-related crime (Sieber 1998; Stephenson 2000), computer-facilitated crime,[19] computer misuse,[20] computer abuse,[21] computer mischief,[22] computer break-in,[23] computer sabotage (Sieber 1996), computer espionage,[24]

---

[18] Computer crime is the most frequently used term in denoting the phenomenon. For example, there is an institution named the "Computer Crime Research Centre". See the institution's Web site, at http://www.crime-research.org/.

[19] See Computer Crime and Intellectual Property Section (CCIPS), Prosecuting Crimes Facilitated by Computers and by the Internet, last modified 15 March 2007. Retrieved 15 February 2016, from http://www.usdoj.gov/criminal/cybercrime/crimes.html.

[20] For example, the usage of this term in "The U. K. Computer Misuse Act 1990 (c. 18)."

[21] For example, the usage of this term in "The US Computer Fraud and Abuse Act (18 USC 1030)."

[22] See, for example, Woodward, C. Washington Quarter Voting Hijacked by Computer Mischief, Associate Press, 10 April 2006. Retrieved 15 February 2016, from http://seattlepi.nwsource.com/local/6420AP_WA_State_Quarter.html. In unofficial English translation (by the Finnish Ministry of Justice) of the Penal Code of Finland, Chapter 34, Section 9a (578/1995) defines criminal computer mischief, stating that "A person who, in order to cause harm to automatic data processing or the functioning of a data system or telecommunications system, (1) produces or makes available a computer program or set of programming instructions designed to cause harm to automatic data processing or the functioning of a data system or telecommunications system or to damage the data or software contained in such a system, or distributes such a program or set of instructions, or (2) makes available guidelines for the production of a computer program or set of programming instructions or distributes such guidelines, shall be sentenced, unless an equally severe or more severe penalty for the act is provided elsewhere in the law, for criminal computer mischief to a fine or to imprisonment for at most two years."

[23] In unofficial English translation (by the Finnish Ministry of Justice) of the Penal Code of Finland, Chapter 34, Section 8 (578/1995) defines criminal computer mischief, stating that "(1) A person who by using an unauthorized access code or by otherwise breaking a protection unlawfully hacks into a computer system where data is processed, stored or transmitted electronically or in a corresponding technical manner, or into a separately protected part of such a system, shall be sentenced for a computer break-in to a fine or to imprisonment for at most one year. (2) A person shall also be sentenced for a computer break-in if he, without hacking into the computer system or a part thereof, by using a special technical device unlawfully obtains information contained in a computer system referred to in (1). (3) An attempt is punishable."
(4) This section applies only to acts that are not subject to an equally severe or more severe penalty provided elsewhere in the law.

[24] Defence Investigation Service, Computer Espionage, The American Report, number

computer manipulation (Sieber 1996), etc. "Comcrime" was used in the title of Sieber (1998), though the term was not used in the main body of the text.

The second group of terms are accompanied with a crime particularly facilitated by computer networks. The origin of the term "cybercrime" cannot be identified, but there is no doubt that it became prevalent with the legislating process of the European Convention on Cybercrime. The prefix "cyber" simply means computer, but people tend to use it in terms of networked computers. Generally, people wish to distinguish the criminal phenomena in the network age from that before the 1990s. Smith, Grabosky and Urbas (2004, pp. 5-6) have argued that "cyber" used as an adjective does not equal to "cyber-" used as a prefix. That is to say, "cyber crime" is not "cybercrime". They have used the term "cyber crime" "to describe a range of criminal offences, only some of which specifically relate to computers and the telecommunications infrastructure that supports their use." (p. 5) They have viewed "cybercrime" as "a singular concept of crime that can encompass new criminal offences perpetrated in new ways" and "cyber crime" as "a descriptive term for a type of crime involving conventional crimes perpetrated using new technologies." (p. 6) Most authors are using these two terms interchangeably. Besides terms cybercrime, or cyber crime, people also use net crime,[25] the Internet crime (Taylor and Quayle 2003), crime on the Internet,[26] Internet-related crime,[27] network crime,[28] etc. In Finland,

---

288, 5 May 1996. Retrieved 15 February 2016, from http://www.kimsoft.com/korea/edispy.htm; McNamara (2003).

[25] For example, the term net crime was used in news report, Luening, E. European Council Moves Net Crime Treaty Forward, CNET News, 20 November 2000. Retrieved 15 February 2016, from http://news.com.com/2100-1017-248874.html

[26] For example, Darlington, R. Crime on the Internet. Retrieved 15 February 2016, from http://www.rogerdarlington.co.uk/crimeonthenet.html

[27] For example, Computer Crime and Intellectual Property Section (CCIPS), How to

cybercrime is sometimes translated as "tietoverkkorikos" (information network crime), with the same meaning as "tietotekniikkarikos" (information technique crime), referring to both offences targeting information processing systems and offences committed with the assistance of information processing systems.[29] According to Darlington (n.d.), crimes on the Internet include "hacking, viruses, pirating, illegal trading, fraud, scams, money laundering, prescription drugs, defamatory libel, cyber stalking, cyber terrorism." According to CCIPS (2006), Internet-related crimes include "computer intrusion, password trafficking, copyright piracy, theft of trade secrets, trademark counterfeiting, counterfeiting of currency, child pornography or exploitation, child exploitation and Internet fraud matters that have a mail nexus, Internet fraud and spam, Internet harassment, Internet bomb threats, trafficking in explosive or incendiary devices or firearms over the Internet."

The third group of terms regard the Internet as only a part of the whole telecommunications systems.[30] Electronic crime (e-crime) emphasizes the characteristic of the criminal phenomena relating to (micro) electronics rather than to computer or computer networks. "The term 'e-crime' arose in the tradition of terms such as e-mail, e-commerce, e-zines, e-tailer and e-

---

Report Internet-Related Crime, Last modified 15 March 2007. Retrieved 15 February 2016, from http://www.usdoj.gov/criminal/cybercrime/reporting.htm

28 In Chinese, the counterpart of the term cybercrime is simply "wangluo fanzui" (network crime).

29 Governmental Proposal HE 153/2006 of Finland concerning Approval of Council of Europe Convention on Cybercrime (here after HE 153/2006), General Justifications, 1. Introduction.

30 For example Tennyenhuis and Jamieson (2003), pp. 187-206; Australian Police Commissioners' Conference Electronic Crime Working Party of Australasian Centre for Policing Research (2000), The U. S. Technical Working Group for Electronic Crime Scene Investigation (2001), etc.

government."[31] With this term, people usually indicate the same phenomenon as cybercrime, but others also extend it to cover crimes relating to the telecommunications systems, in which the Internet is only a part of the whole systems.

The fourth group of terms regard the space, the community, or the environment created by the Internet as the place where a crime is committed. The word "virtual" has a deep and different meaning in the term "virtual reality",[32] but "virtual crime" is in fact the substitute of cybercrime in the sense that the crime is committed in the network environment. A purely virtual crime has not been criminalized.[33] When used as synonym for cybercrime, the focus of the term "virtual crime" is put into the specific spatiotemporal context created by the Internet and interpersonal communication via the Internet.

The fifth group of terms regard the data, information or privacy as the primary factor in a crime. In fact, cybercrime is crime related to information or information systems (not limited to computer and computer networks). Future terminology should therefore incorporate information or information systems into the name of such a crime.

The sixth group of terms regard the processing of "digital" information as the unique characteristic of cybercrime (Lilley 2002). "Digital" means "using a system in which information is recorded or sent out electronically in the form of

---

[31] See McKenizie, S. What are Electronic Crimes? 2 July 2004. Retrieved 15 February 2016, from http://www.criminology.unimelb.edu.au/research/ecrime/ecrimedefn.html

[32] Virtual reality indicates an environment produced by a computer that looks and seems real to the person experiencing it. See Summers (2003), p. 1841.

[33] Such as the case of "a rape in cyberspace" described in Dibbell (1993). The article described a "cyberrape" performed by a Mr. Bungle in a multi-user dungeon (MUD), called LambdaMoo, and the repercussions of his act. See Wikipedia, A Rape in Cyberspace, 17 April 2006. Retrieved 15 February 2016, from http://en.wikipedia.org/wiki/A_Rape_in_Cyberspace.

numbers, usually ones and zeros."[34] Digits are neither the system through which the crime is committed, nor the technology by which the crime is committed. Rather, they are the form in which information is processed through the system. A crime can hardly be "digital" because the committing process of a crime differs from the processing form of information.

The seventh group of the terms regard ICT as high technology. A crime involving ICT is named high technology crime,[35] high-tech crime,[36] hi-tech crime,[37] or information technique crime.[38] In fact, the term "high technology" is only used to indicate modern high technology, excluding the ancient ones. In the viewpoint of the tenth century, papermaking may be a high technology. In the viewpoint of fourteenth century, movable type printing technique may be another high technology. They can both be regarded as technology relating to information processing. This indicates that the term high technology is unsuitable for naming a crime. On the other hand, most computer-related

---

34 See Summers (2003), p. 436.

35 Kovacich and Boni (1999); the International High Technology Crime Investigation Association. "(HTCIA) is designed to encourage, promote, aid and effect the voluntary interchange of data, information, experience, ideas and knowledge about methods, processes, and techniques relating to investigations and security in advanced technologies among its membership." Retrieved 15 February 2016, from http://www.htcia.org/aboutus.shtml

36 For example, an institution named "Australian High Tech Crime Centre", which "employs representatives from all Australian State and Territory police forces in both its staff and its Board of Management. This creates an environment of cooperation and national consistency to referrals, training, education, intelligence, policy and investigations." See web site, at http://www.ahtcc.gov.au/.

37 For example, an institution named "The National Hi Tech Crime Unit", which is part of the Serious Organised Crime Agency, see web site, at http://www.nhtcu.org/

38 For example, in Finnish, the literal meaning of the term "tietotekniikkarikos" is information technique crime. The term is used interchangeably with "tietoverkkorikos" (information network crime) (HE 153/2006, General Justifications, 1. Introduction). The general understanding of cybercrime is that it happens in the environment of information processing systems and with an expertise on the operation of such systems (Ibid).

crimes have in fact only used "low tech" as Molnar (1987, p. 714) found in his study. Therefore, there has been a misunderstanding in giving the general public the impression that each and every kind of computer crime is sophisticated and not committed by ordinary person (ibid).

2.5 Reading of the "cyber" label of criminal phenomenon

As noted, the prevalence of the prefix "cyber" readily becomes a substitute for the terms computer and computer network. Anything can be "cyber" if it is related to the computer and the computer network. Cybercrime is not always a crime that did not exist in the pre-computer era, just as we cannot deny the existence of "ancient" white-collar crime before Sutherland coined the term. The twentieth century was the time when people tended to label old or new things with new inventions. The most apparent example is the use of the word "modern." Due to the overuse of the word, people today cannot use the word modern any more. Criminal law and criminology are also full of labels of this kind.

One of crime's labels currently in use is "cyber." To label a crime "cyber" has a similar meaning to labelling the present historical period as an information age. In addition, it has a further significance in criminology. The following analysis is only an effort to explore the subtext to which the prefix "cyber" can refer.

(1) The label contains the implicit meaning of deviant behaviours dependent on information systems. Violent crime is a label for deviant

behaviours involving the use of human force. Intelligent crime is a label for deviant behaviours involving the use of wisdom. White-collar crime is a label for deviant behaviours by the perpetrator's occupation. Similarly, cybercrime labels deviant behaviours that depend on information systems, without which the offences are impossible to commit, or by which the offences may be committed more efficiently.[39] The more the people are heavily dependent on information systems, the more the offences that cannot be committed without such systems are committed; the more the offences with such a system can be committed more efficiently the more frequently they occur. The prefix "cyber" is meant to characterize the dependence of new types or new categories of offences on information systems which label this society.

(2) The label sketches the semi-virtual and semi-real crime scene. Many people are talking about a different space as virtual. In fact, due to technological limits, perfect virtual space has not been realized. The current cyberspace is a semi-virtual and semi-real space. Thus, pure virtual interaction is neither possible nor has its meaning. The information age is a term merely symbolizing a developing stage of virtual space, a partly virtual and partly real environment. Naturally, cybercrime only involves a semi-virtual and semi-real crime scene. It is true that the supposed neural computer may construct a pure virtual atmosphere and facilitate a pure virtual crime. However, the virtual crime scene cannot appear before a robot driven by a neural computer is created.

---

[39] There is no a lack of viewpoints that regard computer crime as a kind of white-collar crime. For example, Bequai (1978, p. 1) stated: "Computer crime is part of a larger form of criminal activity –white-collar crime." Considering that the concept of white-collar crime is becoming vague in the information age, this study generally does not classify cybercrime into the bigger category of white-collar crime.

(3) The label gives us an impression of human-machine criminal interactions. Human-machine interaction represents only a piece of social interactions. The results of human-machine interaction can be human-machine-human or human-machine-machine interactions. The process can be unlimitedly expanded. Furthermore, the participants in the interaction can be multiple humans and multiple machines, that is, in networked systems. This shows the complicacy of online activities including cybercrime.

In fact, the human-machine interaction has a deep impact on the criminalization of deviant behaviours relating to information systems. For example, in the Governmental Proposal HE 153/2006 (Finland), the spreading of computer virus has been noted as likely to be realized through delivering it to other persons, or to be through spreading it in the machines.[40]

(4) The label demonstrates on extension of the criminal territory. The traditional crime happens in the visible sphere and is mostly territory-dependent. In the information age, the territorial extension of crime has dual meanings. On the one hand, the criminal phenomenon extends from the visible sphere to the invisible sphere. Cybercrime generally crosses both visible and invisible spheres simultaneously. The process and results of cybercrime are both revealed only with difficulty. On the other hand, trans-territorial crime becomes easy with the help of information systems, as compared with the traditional communications system and transportation system. Information systems integrate the function of many traditional systems, enabling a remote operation of communications, transportation, authentication, banking, printing, and so forth.

---

[40] HE 153/2006, Detailed Justifications, 3. Reasons of Governmental Bills, 3.2 Penal Code, Chapter 34 Endangerment.

(5) The label causes multidisciplinary attention. In the past, scholars attempted to label all those disciplines relating to crime by the term "criminal" and formed many marginal disciplines, such as criminal psychology, criminal sociology, etc. The twentieth century development of criminal phenomena made it overcomplicated to create so many disciplines. Rather than labelling informatics, cybernetics, etc., "criminal", scholars from different disciplines pursue research from their own standpoints. Works of many disciplines accommodate the contents of cyber ethics and cybercrime as inseparably constituent. Crime and its study are both more "cyber" than "criminal". Many criminalists migrated from the criminal sciences to other disciplines before the information age. Today, more non-criminalists are migrating from their own disciplines to the criminal sciences.

(6) The label holds the digital criminal power. While information systems utilize the power of the digital form, crime is also becoming digital. "Being digital"[41] means "being different" from the traditional social life. "Being digital" also means complexity and advancement of criminal circumstances. The power of information is expressed in digital form, both in social welfare and in social problems. It is natural for criminals to exploit the digital power of the scientific and technological advancement. In fact, the criminal phenomenon of the present day is modernized by the label of "being digital" in its spatiotemporal existence, with the emergence of new types of offences and new forms of old offences.

---

[41] "Being digital" comes from the name of a book by Nicholas Negroponte (1995), who put forward a future vision of digital technology.

(7) The label does not disrupt the vitality and continuity of the criminal tradition. Aggressive activities are universally acknowledged among animals. Crime is as old as human beings, finally imposed punishment by law. The corner-stones of criminal science are offences such as homicide, theft, robbery, arson, etc. The development of criminal phenomena demonstrates the continuity of tradition and the revision of minor details, including the tools used, the vehicle driven, the assets obtained or the premises destroyed. However, with interests and security as the basic goals, the foundation of criminal phenomena has not changed. Labelling a crime "cyber" is merely adding new factors to the tradition, but not undermining the innate foundation. With this label, traditional criminal law just takes a new step forward.

(8) The label confirms the transformation of criminal patterns. If we say that the traditional criminal phenomenon was symbolized by forces and violence, the characteristic of cybercrime is the involvement of intelligence and intrigue. The physical and psychological existence of past human beings was confronted by threats of starting a bloody scene. Even in the present day, terrorist attacks are far more often the primary headlines in the mass media and a theme of critical concern for governments. For example, in 2005, approximately 11,111 terrorist attacks occurred and resulted in over 14,602 killed, 24,705 injured, and 34,780 kidnaps. Approximately 630 attacks accounted for over half of the total fatalities.[42] In 2014, totally 13,463 terrorist attacks occurred in the world, resulting in more than 32,700 deaths and more than 34,700 injuries.

[42] The U. S. Department of State, Country Reports on Terrorism, 2006, Statistical Annex, v and vi.

Furthermore, more than 9,400 people were kidnapped or taken hostage.[43] The bloody scene remains a severe threat, but a silent transformation of this threat is happening with the continuing growth of information systems. Certainly, there is no sign demonstrating that the traditional fatal violence can be replaced by cybercrime or cyber terrorism. Cybercrime represents merely a tip of the iceberg of the entire crime scene. We still doubt whether the hacker will be the future captor or killer?

2.6 The necessity of a broad definition of cybercrime

Considering the previous experiences and lessons in legislation and law enforcement, I strongly advocate a broad definition of cybercrime, which would then have a number of advantages in criminal-law reform.

First, a broad definition of cybercrime would help to achieve as great a consensus as possible in the context of criminal-law reform. International negotiation is a prolonged and expensive process, a consensus based on a narrow definition would not be as effective as one based on a broad definition. Criminal justice according to a less consentient mechanism will inevitably meet unsolvable difficulties that require a new round of international consultation. Considering that current international consensus is inadequate, supplementary agreement is necessitated in the near future to acquire a broader coverage. An international treaty should be based on such a broad definition that member

[43] The U. S. Department of State, Country Reports on Terrorism, 2015, Annex of Statistical Information.

states would only exclude *by way of reservations* clauses unsuitable according to their own needs and traditions, but not exclude such contents from the treaty and hinder other state from accepting these clauses.

Secondly, a broad definition would help to revise criminal law completely, thus avoiding merely adding simply a couple of isolated articles. The isolated articles leave the cybercrimes in the broad sense unpunishable according to laws. The broader the coverage of the definition is, the more possible it is for criminal laws to prescribe more activities as falling under the category. Many countries, including China and the U. S., initially passed laws with very limited coverage over activities or targets; however, they all subsequently made amendment so as to expand the scope of their legislation. Starting from a broad definition will avoid the waste of legislative resources.

Thirdly, a broad definition would help to amend procedural criminal law based on substantive criminal law. Without a qualified procedural law, the amendment of substantive law is easily invalidated. In the common-law system, the division between procedural law and substantive law is not so clear. Nevertheless, in other legal systems, the coordination of these two branches of law has sometimes required a special legislative process. The prior enactment of substantive law is reasonable before procedural law. For both the substantive and procedural laws to be more effective and more consolidated, a broad definition of cybercrime would enable a better drafting of provisions in procedural law.

Finally, a broad definition would also help to provide full protection for a critical information infrastructure. Legal science should always face the social changes that are seeking to influence legal notions and the legal framework.

However, social changes have never happened so rapidly in the history they do as today. The development of cybercriminal phenomena is a particular example that must be considered from the global view. In less developed or less rapidly developing countries, their laws cannot wait for the occurrence of cybercrimes within their own boundaries. Every offence existing in other countries may cross the borderless networks without perception.

2.7 A definition based on roles of information systems

In this book, cybercrime is defined as any type or any form of traditional or untraditional crime involving information systems in use as media, means, place, route, target, tool, or used in the preparation for other crimes.

First, cybercrime covers any form of traditional or any type of untraditional crime that can involve information systems. With the universal use of information systems, many types of new crimes emerge, many old crimes occur in new forms, and many new and old crimes happen interlinked. If information systems are the key factors in the crime, the crime falls into cybercrime. If an offence cannot be committed through information systems, it is not a cybercrime. According to the relationship between the cybercrimes and traditional crimes, cybercrimes can be divided into cybercrimes as substitutes for traditional crimes and cybercrimes as the complements of traditional crimes. The occurrence and increase of substitutes depend on the costs compared with the traditional crimes. When the costs of cybercrimes are lower than traditional crimes, cybercrimes will increase, vice versa. The occurrence and increase of

complements, nevertheless, depend on the costs when compared with traditional crimes committed by other means. When costs of traditional crimes committed by the means of computers and networks are lower, crimes of this kind will increase, vice versa. In this sense, cybercrimes turn out to be traditional crimes facilitated by computers and networks.

Second, information systems are the distinct factor in cybercrime. Li (1993) proposed that a computer crime should be defined as a crime relating to "computer information systems". Computer crime, or cybercrime, is by its nature information crime. The definition of cybercrime must contain the element of digital information or be a part of information systems. But computers and networks are simply the *present* representative of information systems to create, process, transmit, duplicate, exchange, disseminate, modify and destruct digital information. The hardware, software, and peripheral devices are only parts of these information systems. The development of ICT may simply outgrow the systems' current forms. Whatever the forms we use, however, such a mechanism as information systems will remain.

The terms "computer" or "network" cannot embody the complete scene of information systems, nor be expected to point out necessarily to the future of the technology. Many of the previous definitions focused on "computer"; and later definitions emphasized "network" as well. However, the image of computers and networks is changing; the transformation in the future may be faster and greater. It is reasonable to incorporate the term of "information systems" into the definition of cybercrime instead of using the terms of "computer" or "network".

Thirdly, information systems must be in use. Information systems not in

use cannot facilitate a cybercrime. The term "in use" has to be understood in a broad sense. A computer is in use from the time it is purchased as a facility until the time when it is disused and disposed as cast-off. The transportation, installation, debugging, examination, reparation, and temporary switching off do not cancel the status of being in use. A paid order is enough to make a computer in use, because the expected use will influence the decision-making and productivity of the user. If such a computer were to be damaged and the schedule of adopting such a device delayed, or the expected benefit reduced, the loss of the user would be apparent. A network in use also has a similar meaning. Different stages in the whole process of being in use have a similar sense but are different in importance.

In some cases, however, computers are no more than entertainment equipment in a victim's daily life. Where this is the case, the function of the information processing of the computer is not particularly emphasized. Then, even if the computer is quite valuable, theft or destruction of it should not be regarded as a cybercrime. In KKO:2000:17, the accused, who was invited to the victim's house, took the victim's portable computer and other devices after the victim fell asleep. In I-SHO 13.11.2006 1401, the accused usurped a portable computer valued at 880 euros from a shop and sold it to a man at the price of 70 euros, for he regarded it as a typewriter. Although the movable property was valuable, nothing about the special function of the computers was mentioned in the courts. It is apparent that the offence was not committed against information systems "in use" for the purpose of information processing, and the loss was of such a nature as to be neglected compared with the value of the computers as commodities.

Fourthly, the roles of information systems in cybercrime are multiple. Information systems can be exploited as media, means, place, route, target, tool of a crime, or used in the preparation for other crimes. Exactly as explosives are different from primitive weapons, a plane different from other vehicles, information systems are different from many traditional facilities. The accompanying conceptions are data processing and transmission, multimedia, virtual reality, remote control, online interactive, and so forth. With information systems, people are involved in intersensory actions. To highly evaluate the functions of the (current and future) information systems is a matter that cannot be overestimated. The equivalent applies to the situation of cybercrime, which is committed intersensorily.

Finally, it is also necessary to point out that, even if we adopt a broad definition of cybercrime, the offences merely involving information systems but having nothing to do with their functions do not constitute cybercrime. A typical example is the prohibition of import or export of computers, software, or technology. Many countries have trade prohibitions of this kind so as to maintain the political, military, or scientific competitive priority, and this might mean even limiting the public from using such devices. For example, according to the Myanmar Computer Science Development Law of 1996, the importing or keeping in possession or utilizing any type of computer, or setting up a computer network or connecting a link inside the computer network, without prior sanction, are offences punishable by imprisonment of 7 to 15 years and a fine. Offences of this kind do not belong to cybercrime in terms of this book.

CHAPETER 3 CLASSIFICATION OF CYBERCRIME

Cybercrimes can be classified under different definitions and according to different standards. Scholars have proposed numerous plans for categorizing cybercrimes. For example, Bequai (1979a, pp. 106-107), who originally regarded cybercrime as part of white-collar crime, proposed to classify computer crime into five categories, including vandalism, theft of information, theft of services, theft of merchandize or other property, and fraud. Bequai (1983) thereafter developed his classification into seven categories, including financial thefts, frauds, and abuses; thefts of property; abuses of data; unauthorized use of services; vandalism; sabotage, and political and industrial espionage (pp. 17-21). Wasik (1991, pp. 41-60) proposed six categories of computer misuse, including unauthorized access, computer fraud, unauthorized removal of data or programmes, unauthorized use of computer time or facility, and destruction and damage. Wasik (1991, pp. 24-33) put forward three levels of relationships between the conceptions of computer crime and white-collar crime: (1) corporate crime, (2) occupational crime, and (3) misuse committed by outsiders. To a certain extent, this can also be regarded as a classification system. Grabosky (2000) considered nine varieties of cybercrime, including theft of services, communications in furtherance of criminal conspiracies, information piracy and forgery, the dissemination of offensive materials (including extortion

threats), electronic money laundering; electronic vandalism and terrorism; telemarketing fraud, illegal interception, and electronic funds transfer fraud (pp. 3-8). Icove and co workers (1995), Sieber (1996), and many other scholars have also proposed various methods of classification. An exhaustive bibliography is neither necessary nor possible. However, this section will present a classification method according to the roles that information systems play in offences.

Many earlier definitions of computer crime have already contained some methods of classification based on the different roles of the computer in offences. The development process is from simple categories to complex categories. The earliest definition contained the only category, that is, crime by computer (for example Parker 1976). A subsequent definition contained two categories, that is, crime by computer and crime against the computer.[44] MacKinnon (1997) classified cybercrime into computer-incidental crimes and computer-instrumental crimes, and defined computer-incidental crimes as offences in which the computers are merely used "incidentally or tangentially"; computer-instrumental crimes involve computers more "directly" as the "tool" or instrument (MacKinnon 1997, p. 210). The U. S. Department of Justice (2000) categorized computer crime into crimes in which computers are targets, storage devices, and communications tools. Parker and Nycum (1984, pp. 313-314) identified four ways of committing criminal acts with computers, that is, the computer as the object, subject, tool of the crime, and the symbol of the

[44] In the network environment, scholars have also transplanted this category in their research on cybercrime. Casey (2000), as cited in Levinson (2002), p. 455, saying that cybercrime can be a traditional crime that is committed through the use of a computer or the Internet, or a crime that involves particularly the targeting of computer technology.

computer used in intimidation or deception. Carter (1995) divided computer crimes into four categories, including offences in which the computer was the target; the computer was the instrument of the crime; the computer was incidental to other crimes; and crimes associated with the prevalence of computers. Whereas information systems play an increasingly essential role in contemporary society, considering that the offences accompanied by information systems are being increasingly diversified, we feel that there is a need to expand the categories of cybercrime with regard to information systems. In discussing digital extortion, Grabosky (2000) has listed the roles of information systems as media for threat, targets of threatened action, media for disclosure of embarrassing personal details, means of facilitating payment, and incidental to the offence (pp. 34-50). In recent year, research in actual happenings of cybercrime also listed cybercrime according to survey result. For example, a survey concerning incidents of computer crime in German companies in 2015 found the following (Statista 2015):

Figure 1 Types of Cybercrime in Germany

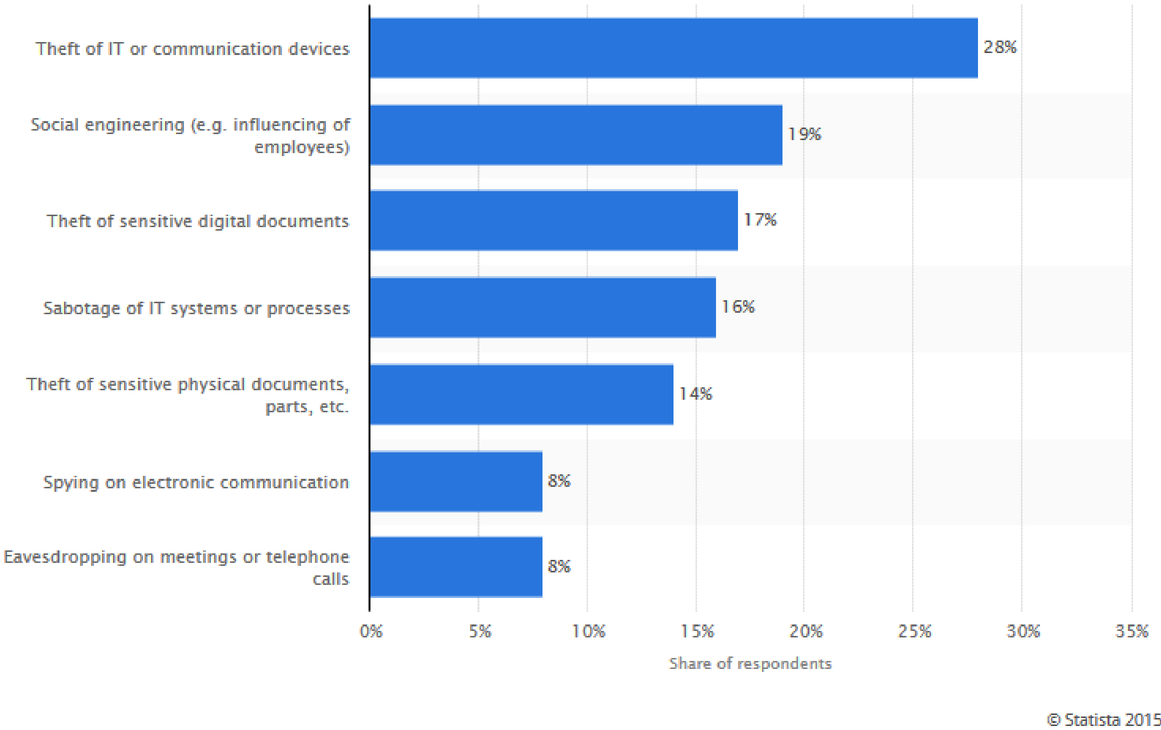


Table 1 Cyber Threats of Most Concern in Australia

• 72% — ransomware or scareware
• 70% — theft or breach of confidential information
• 67% — targeted malicious emails
• 66% — advanced persistent threats (APTs)
• 62% — unauthorised access to information from an outsider
• 58% — social engineering
• 56% — unauthorised access to information from an insider
• 55% — loss or destruction of information
• 54% —loss of service ability
• 52% —virus or worm infection
• 46% — trojan

• 46% — unauthorised modification of information
• 40% — theft or loss of intellectual property
• 40% — rootkit malware
• 36% — denial of service attack
• 32% — compromise of mobile devices and laptops
• 24% — wire fraud
• 22% — theft of mobile devices and laptops
• 7% — other

(The percentage means the rate of respondents' answer to the question about the cyber threats and actors of most concern to their organisation. Source: Australian Computer Emergency Response Team. 2015, p. 22.)

All these discussions prove that information systems can play a variety of roles and can be differently targeted in offences.

In the following sections, the roles of information systems in cybercrime will be expanded and cybercrime will be divided into seven categories. Information systems can be target, tool, media, route, place, and means of crimes and can be used in preparation for other offences. In previous literature, the dichotomy recognized the roles of information systems used to be summarized as target and tool (or termed instrumentality). The term "tool" or "instrumentality" has been used in an unlimited broad way. In practice, the roles that information systems can play are far more abundant than merely being a tool or an instrumentality.

3.1 What roles can information systems play in cybercrime?

3.1.1 Information systems as targets

"Computers are targets" is a subtitle in Bequai (1983, pp. 7-11). At present, we can roughly assert that the whole information systems are targets. In a certain sense, information systems can be regarded as networked assets (Wells and Sevilla 2003), including tangible assets and intangible assets, hardware and software, intra-national assets and international assets. Networked assets are a kind of combinative assets existing in cyberspace. Furthermore, networked assets are dynamic, existing in the process of production, which constitutes a kind of production management, for example, covering activities that can be included in the field of electronic commerce.

The economy, national security, politics, military affairs, science and technology, education and medicine increasingly depend on the Internet, through which information is created, stored, transmitted and processed. When information security is threatened, the whole country will suffer great losses.

The Internet is vulnerable to artificial attacks, some of which belong to traditional crimes, for example, cutting off the electricity supply, destroying cables, moving antennae used in satellite communications; and more traditional crimes, for example, destruction of computers and peripheral facilities.[45] Nowadays, these actions are not uniformly regarded as cybercrime. Cybercrime against the Internet mainly exploits computer technology. The most typical attacks are through computer viruses and other malicious programmes. There

---

[45] These were regarded as computer crimes in books published several years ago. For example, Icove and co-workers (1995), saying that "Terrorist bombings on buildings housing computer equipment, arson, and theft and destruction of computer equipment fall into this category."

has already been a long list of instances of serious viruses.

In fact, sometimes computers and networks have the nature of both instrument and target. For example, an attack on the Internet must be launched through the Internet itself. As mentioned above, these classifications are not mutually exclusive. Rather, they can be carried out in a compatible way. The perpetrator's Internet resources are more likely to be used as instruments, while that of the others are more likely to be aimed at as targets. The Internet is, however, composed of huge indivisible systems that can be both exploited or attacked.

It should be emphasized that, "the stealing of computers, computer chips and other computer equipments from commercial premises" as in R. v. Kehoe and Others,[46] might seem not so relevant to our discussion at first glance. However, a natural result of these activities is that a computer-aided business and computer-processed data may be damaged, and thus it remains a cybercrime in our sense. Taking into account the disabling of the functioning of whole information systems, and the loss of information in internal memory media, thefts of computers and their parts represent more than illegal access to the systems and information. For instance, in Investigation into Security of Personal Information Held by Vancouver Coastal Health Authority's Employee and Family Assistance Programme, the thief stole from the office of manager of the administration a desktop computer containing a database of approximately 11,000 clients.[47]

---

[46] It has been dubbed a "highly sophisticated and successful criminal enterprise," what one of the perpetrators confessed as that "Computer crime is what I do." [1998] EWCA Crim 1163 (1st April, 1998). See also Section 6.3.

[47] Investigation into Security of Personal Information Held by Vancouver Coastal

A different situation appeared in R. v. Moseley,[48] where the victim was robbed of property, including "computer and electrical equipment, a rucksack and a personal organiser, and cash cards." In THO:2005:28, two portable computers were found at the accused's two residences. The charge and the conviction against the perpetrator mentioned nothing about the particularity of the computer and the information inside it. The computer here is nothing more than a target of traditional robbery—no information systems were interrupted, and no information was destroyed or disclosed.

In addition, the term information systems is used here in a broad sense as referring to information systems and the information in them. In practice, these two conceptions are usually used separately. For example, in the U. K., the Computer Misuse Act 1990 has been assigned the principal function of defending the integrity of the systems but not of information, while the latter task falls on the Data Protection Act 1984.[49]

Offences in which information systems are targeted roughly cover:

1. Unauthorized access to information systems,[50]

2. Unauthorized access to information,[51]

Health Authority's Employee and Family Assistance Program, Re, 2006 CanLII 20511 (BC I.P.C.).

48 [1999] EWCA Crim 1089 (21st April, 1999).

49 DPP v. Bignall [1997] EWHC Admin 476 (16 May 1997)

50 This has been criminalized by Convention on Cybercrime, Article 2; the Danish Penal Code Article 263, Section 2; the Finnish Penal Code Article 28; the Swedish Penal Code, Chapter 4, Section 9c. In United States v. Sablan (Ninth Circuit No. 94-10533, D. C. No. CR-94-00017-JSU, 7 August 1996), the accused has recently been dismissed from a bank. After some drinking, she used a key she had kept and went to her former work site, where she used an old password to log into the bank's computer, modified or deleted several files, and then logged off.

51 In legal instruments, illegal access to information system and illegal access to the information in the system are usually linked together, neglecting their obvious difference. In the Convention on Cybercrime, Article 2, illegal access to information

3. Unauthorized alteration of information,[52]

4. Unauthorized interruption of information systems,[53]

5. Attack by viruses, worms, logic bomb, Trojan horse, and other malicious programmes,[54]

6. Theft of computer time, network time, or telecommunications services, a specific form of illegal access,

7. Possession, disclosure and providing unauthorized persons with unauthorized information; or unauthorized possession, disclosure and providing unauthorized persons with information, both being the extension of

---

was the purpose of illegal access to an information system. A similar provision is seen in the Danish Penal Code Article 263, Section 2. the Finnish Penal Code distinguishes between these two acts, dealing with illegal access to information in Article 38. See also the Swedish Penal Code, Chapter 4, Section 9a. In United States v. Czubinski (First Circuit No. 96-1317, 21 February 1997), the court reversed the original conviction, which was based on the accused's "unauthorized browsing of taxpayer files" with his valid password, even though he was required to access only accounts needed to accomplish his official duties.

52 Convention on Cybercrime, Article 4, providing computer-related fraud through inputting, altering, deleting or suppressing computer data, interfering with the functioning of the computer system. It covers both alteration of information and influence on the information system. See also the Danish Penal Code, Article 291; the Finnish Penal Code, Articles 33 and 35; the Swedish Penal Code, Chapter 12, and when the acts involve public danger, Chapter 13, Sections 4 and 5. In United States v. Magnuson (Fourth Circuit No. 964957, D. C. No. CR-96-186-A, 24 June 1997), the accused used his home computer to intrude into and disable the victim's computer servers in seven states.

53 Convention on Cybercrime, Article 5. See also the Danish Penal Code, Article 193; the Finnish Penal Code, Article 35; the Swedish Penal Code, Chapter 12, and when the acts involve public danger, Chapter 13, Section 4 and 5.

54 Convention on Cybercrime, Article 6. See also Danish Penal Code, Articles 193 and 291; Finnish Penal Code, Articles 33 and 35; Swedish Penal Code, Chapter 12, and when the acts involve public danger, Chapter 13, Sections 4 and 5. In United States v. Sullivan, (Fourth Circuit No. 01-4330, 25 January 2002), the perpetrator planted a logic bomb into the software prepared for the company before he quit. Four months later, the logic bomb disabled hundreds of hand-held computers used by the company's sales representatives to communicate with headquarters.

illegal access to information.[55]

8. Unauthorized interception of communications.[56]

3.1.2 Information systems as tools

The offences in which computers and networks are utilized as tools have the longest history in computer crime (Parker 1976; Bequai 1978). Networks are widely interconnected outside the limits of time and the boundary of space. As society is becoming more dependent upon computer data processing and the telecommunications systems. With the Internet, crackers intrude into others' computers, web sites, e-mail accounts of individual and organizational users whose data, secrets, privacy and electronic property are stored there.

Under these circumstances, the Internet is becoming the instrument by which perpetrators commit not only traditional crimes but also new crimes. It is not only the instrument by which people commit crimes, but also the instrument through which people are victimized. In using the Internet, some people unwittingly break the law, while others are unwittingly harmed by crimes. Definitely, under more circumstances, perpetrators intentionally use the Internet to commit criminal acts. Therefore, the crackers who intrude into

---

[55] In the United Sates v. Pitts (Fourth Circuit No. 97-4616, 28 January 1999), the accused, who "was trusted with access to very sensitive and highly classified materials related to counterintelligence operations, surveillance of Soviet officials assigned to the United Nations, and the true identities of American agents and Soviet defectors", "attempted to provide or made preparations to provide his undercover FBI handlers with computer diskettes containing information classified as 'Secret'..."

[56] Convention on Cybercrime, Article 3. See also the Danish Penal Code, Article 263; the Finnish Penal Code, Article 38; the Swedish Penal Code, Chapter 4, Section 8.

others' cyberspace through wired or wireless connections to the Internet are violating others' privacy, plundering others' data, stealing others' secret information, and embezzling others' property.

This kind of cyber instrument contains both the similarities and the differences from the traditional instruments. The case where one opens others' e-mails by a password, then marks it as unread and exits, is comparable to the case where someone opens one of the letters of another with a knife, and then seals it with glue. They both constitute an infringement of freedom of correspondence, but the concept of instrumentality is different. The instrument of the Internet bears with it the characteristic of a remote control, in which the criminal is not necessarily present in person at the crime scene where the letters exist, and does not necessarily leave footprints or fingerprints. The traditional notion of crime scene also changes because of this instrument.

Offences in which information systems are used as tools roughly cover:

1. Forgery and counterfeiting,[57]
2. Computer-aided unauthorized copy of software and other copyrighted

---

[57] The Convention on Cybercrime specifies the criminalization of computer-related forgery, as an act committed through inputting, altering, deleting, or suppressing data. In the national domain, these crimes induce no obstacle to applying traditional law, for example, the Finnish Penal Code, Article 33 can be applied to computer-related forgery. For example, in R. v. Lloyd ([1996] EWCA Crim 1744 (17 December 1996)), the accused was found using a computer with programmes for manufacturing compact discs , a compact writer and blank compact discs to replicate computer programmes. In R. v. Boutrab ([2005] NICC 36 (24 November 2005)), the accused used a false passport with the intent of inducing an employee to accept it. In R. v. Adeoye & Anor ([1997] EWCA Crim 1343 (3 June 1997)), the perpetrator used computer programmes to produce credit cards from plastic blanks. In search, "the police found a printout containing 10,000 credit-card numbers produced by a computer programme." In RovHO 12.06.2001 335, the three suspects, with the assistance of the computer, forged identity cards used for the unauthorized users to watch television programmes transmitted by a company.

works,[58]

3. Telecommunication piracy,[59]

4. Fraud using information systems,[60]

5. Password sniffering and keylogging.[61]

3.1.3 Information systems as media

As a form of media, computer networks have their advantages over the

---

58 See for example, R. v. Johnstone ([2003] UKHL 28 (22 May 2003)), in which the accused pirated recordings and made compact discs and audio cassettes. In THO:2006:6, the accused was said to have made, without the permission of the right holder, 381 karaoke CDs in order to make a profit through using them in the karaoke business. In KouHO:2005:11, the co-defendants cooperated to make and sell DVD copies without the permission of the right holders.

59 In United States v. Clayton (Ninth Circuit No. 96-10127, 11 March 1997), "cloning" was practised by the perpetrator to replicate the stolen identification numbers of legal mobile phones with the help of computer software; they were then used to make calls at the expense of the owner of the legal phone. See also United States v. Cabrera (Eleventh Circuit Nos. 98-4432, 98-4434, D .C. Nos. 96-CR-562-DLG, 98-CR-77-DLG, 19 April 1999), where the accused used a small device named "copy-cat" to clone cellular phone.

60 In R. v. Russell ([2001] NICA 45 (12 October 2001)), the accused used a computer identification number and password to access confidential files in the computer system, identifying persons that he considered likely to claim any type of benefit, and gathering names, addresses and national insurance numbers. After this, he passed the information to a co-offender to make false claims for fraudulent benefits. In R. v. Farkas (2006 ONCJ 121, 10 April 2006), the accused made a profit of 45,000 dollars from victims in the U. S., Canada, and England through fraudulently acquiring goods and fraudulently selling them over a period of 18 months via the Internet purchasing and auction. During the fraud, he obtained credit-card information through on-line chat groups and bulletin-board systems. He sold these goods to legal collectors, during which he received money but did not send the goods to the purchasers.

61 In United States v. Ropp (C. D. California, 7 October 2004), the accused placed a keylogging device on the cable that connected the victim's keyboard to her computer's central processing unit, recording and storing what the victim typed with the keyboard. The indictment was dismissed, but the court made it clear how keylogging works.

traditional media. They surpass the limits of time and space, languages and traffic, and political and legal boundaries. The Internet enables people to "upload, post, e-mail, transmit or otherwise make available content that is unlawful, harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, libellous, invasive of another's privacy, hateful, or racially, ethnically or otherwise objectionable."[62] In fact, racist speech, tutorials for killing, raping, arson, bomb-making and even instructions for virus creating, malicious programme writing, and other forms of cyber attacks are widespread on the Internet. Various degree of political incitement, libel, rumour and superstition crowd up to mislead the public, going even further than the traditional media. Many countries are confronted with web sites managed by separatists, dissidents, and international opposition forces. These web sites always publish their opinions that are harmful to their government but beneficial to themselves. Now, information of this kind is being practically exported and imported across national borders at the speed of light.

One of the notable problems is slander, the false statements that come across the innovative online media injuring others' reputations by publishing false statements. The forms of such slander mainly include impersonating others to solicit sex mates, one-night lovers, publicizing others' telephone numbers, and fabricating photos by inserting the photos of other persons into pornographic photos, etc.

In addition, the online content may cause an international concern, such as racist and xenophobic material, that is, "any written material, any image or

---

62 See Yahoo! Terms of Service. Retrieved 15 February 2016, from http://docs.yahoo.com/info/terms/

any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors."[63]

Offences in which information systems act as media roughly cover:

1. Dissemination of obscene material, in particular child pornography,[64]

2. Dissemination of racist and xenophobic material through computer systems,[65]

3. Online false statement about individuals or corporations,[66]

---

[63] Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist and Xenophobia Nature Committed through Computer Systems, Strasbourg, 7 November 2002, Article 2.

[64] In United States v. Slanina (First Circuit, No. 00-20926, 12 February 2002), the accused was convicted of using a city computer to access newsgroups and download pictures of child pornography. In R. v. Kozun (2007 MBPC 7), the accused distributed child pornography through his own personal computer, in which a programme converted the computer into an automated trading centre on the networks. The police found 3522 files (3368 pictures and 154 movies) in his computer that could be considered as child pornography and available for trade. The age-range of the children involved was between 8 months and 14 years. In Alan Joseph Ogilvie v. Her Majesty's Advocate [2001] ScotHC 69 (27th July, 2001), the accused downloaded from the Internet 12,000 images of child pornography onto his first computer and upon its confiscation, he downloaded a further 10,000 images of the same nature into his newly-bought second computer. In the Convention on Cybercrime, Article 9 criminalizes offences related to child pornography.

[65] In the Additional Protocol to the Convention on Cybercrime, Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (2003), Article 3 criminalizes dissemination of racist and xenophobic material through computer systems, Article 4 criminalizes racist and xenophobic motivated threat, Article 5 criminalizes racist and xenophobic motivated insult, Article 6 criminalizes denial, gross minimization, approval or justification of genocide or crimes against humanity, and Article 7 criminalizes aiding and abetting.

[66] Defamation, including libel and slander, can be dealt with either civilly or criminally, in different jurisdictions. In the U. K., many cases have been settled in civil actions, for example, Godfrey v. Demon Internet Limited [1999] EWHC QB 244 (26th March,

4. Indecent exposure,[67]

5. False advertising,

6. Disclosure of confidential information.[68]

3.1.4 Information systems as routes

Cybercriminals can launch attacks from any computer in different jurisdictions. The continued development of techniques and skills for attacks makes it more difficult and complicated to investigate and prosecute these crimes (McConnell International 2000, pp. 1-2). Information systems can be used to transmit various malicious programmes that have the capacity to disrupt, destroy or limit the functions of information systems. For crackers, using software tools installed on a computer in a remote location, can illegally access to computer systems to obtain data, plant viruses or Trojan horses, or

1999) , where the accused party hosting a newsgroup in the U. S. published a piece that was "squalid, obscene and defamatory of" the victim; Robertson v. Newquest (Sunday Herald) Ltd & Ors [2006] ScotCS CSOH_97 (28 June 2006), where the defendant, a newspaper, which had an online edition, in which a notice was considered of a defamatory nature by the plaintiff was posted by a member of public; in Turner v News Group Newspapers Ltd. & Anor [2005] EWHC 892 (QB) (12 May 2005), the co-defendants, including one of the victim's former wives and a newspaper published an article on how the victim pursued sex with strangers in both printed and online forms.

[67] In Robertson v. Her Majesty's Advocate ([2004] ScotHC 11 (17 February 2004)), the perpetrator induced a seven year old girl to dance naked in front of a webcam and lick her private parts in front of said webcam, *inter alia* (paragraph 9).

[68] In Edward Yearly v. Crown Prosecution Service ([1997] EWHC Admin 308 21 March 1997), the perpetrator published confidential information that he obtained by unauthorized access. There have been numerous cases of such a nature in recent years in the U.K., for example, Grimm (2005, p. 598) reported that 140 applications for the National Institutes of Health (NIH) grant had been leaked on to open access web pages.

cause less serious mischief by changing user names or passwords. As to spies, corporations and governments are committing espionage through the superhighway of the world's Internet. Espionage can penetrate the best security systems and the highest levels of management in cyberspace. Pirates, in their turn, can perfectly reproduce and easily disseminate text, audio, video or multimedia works by using digital technology (Grabosky 2000, p. 8). Some web sites are devoted to "charities" of this kind, similar to providing relief for the poor, who cannot afford expensive software, and thus the market of piracy acts as a solution to satisfy these users. The Internet has increasingly been exploited to distribute pirated works, with the development of new file-sharing techniques.

In the case of illegal access to others' web sites, the intruders may view no document, but usually view encrypted or unencrypted documents, obtain documents, read or delete e-mails, reveal documents to others, destroy files and make the systems inoperable, or use others' accounts to connect with the Internet. The attacks on web sites are growing in intensity. According to the data of the previous Alldas web site, forty-seven attackers defaced 72 web sites in 1998, about 430 attackers defaced 1,079 web sites in 1999, about 2,555 attackers defaced 4,394 web sites in 2000, and in the first quarter of 2001, about 667 attackers defaced 4,797 web sites, a number greater than the victimized web sites of the previous year. Among these cases, the first 15 attackers who defaced at least one percent of the defaced web sites, did one-third of the defacement. The first eight top domain names of the mostly defaced web sites were: ".com,"

".br", ".net", ".cn", ".tw", ".org", ".edu", and ".us".[69] Although the similar source is at present unavailable and several years has passed, this old information indicates that the web sites in the Asian Pacific region rather than Europe are the most likely to be defaced.

The computer systems of national defence of various countries are also the primary targets for hackers. In some cases, the passwords of these agencies were successfully cracked, and other secret information was obtained and disclosed.

Offences in which information systems act as a route roughly cover:

1. E-mail bombing,[70]

2. Harassment through electronic communication,[71]

3. Identity theft and cyberstalking,

4. Denial of service attacks (cyber terrorism),

---

69 These data are obtained and calculated from http://alldas.de by the author in 2001. Later the web site became unavailable.

70 For an explanation of e-mail bombing and other e-mail related crimes, see Planet India Website, E-mail Related Crimes, n. d. Retrieved 15 February 2016, from http://cybercrime.planetindia.net/email_crimes.htm. There, the E-mail bombing is defined as "sending a large amount of emails to the victim resulting in the victim's email account (in case of an individual) or servers (in case of a company or an email service provider) crashing."

71 See, for example, R. v. Jonhson (Johnson, R (on the application of) v DPP [2005] EWHC 3123 (Admin) (8 December 2005)), the accused used both traditional mail and electronic means to harass the victim. He searched the home address of the victim through the Internet, and sent letters or e-mails, harassing the victim directly, or sent letters or e-mails to the employer of the victim questioning her conduct, harassing her indirectly. This behaviour not only affected the victim herself, but also her family and others. In R. v. Debnath ([2005] EWCA Crim 3472), the female perpetrator harassed the male victim by sending fake e-mails to his fiancée and employer; by registering the victim on a web site for people with sexually transmitted diseases seeking sexual liaisons; and by setting up a web site, which had fake information detailing alleged homosexual practices by the victim, and so forth. In X v. European Central Bank ((Officials) [2001] EUECJ T-333/99 (18 October 2001)), the perpetrator repeatedly procured through the Internet documents of a pornographic and political nature and, of having sent them to third parties through e-mails, sent his colleague numerous messages through e-mails containing pornographic and ideologically extreme materials, despite the disapproval of the colleague concerned.

5. Distribution of pirated software, books, magazines, audio, video or live performances, etc.,[72]

6. Infringement of industrial secrets and state secrets,

7. Transmission of child pornography.[73]

3.1.5 Information systems as places

In the information age, much of the money, assets, state secrets and personal privacy are transformed into computer data and stored in computers, or circulated through the Internet (Dong and Li 2015). Meanwhile, networks become a giant gallery of pornography, or a gambling house. Networks do not have value orientation, have no culture, have no legal consciousness, but the information stored and the activities taking place are either protected or prohibited by law. Furthermore, the "place" of networks is trans-territorial outside a unified legal system. Aggressions and harm take place at the terminals, which seems to be the only place where the crimes occur.

Factually, this is contradictory brought about by the special characteristic of the "place" of network. When the Internet is used to facilitate gambling,

---

[72] In KKO:1999:115, the accused allowed e-mail users to copy computer programmes from the mailbox. The mailbox could be viewed as a deposit place, but the software was transferred through information systems.

[73] In United States v. Muick (Seventh Circuit No. 97-CR-30004, 8 February 1999), the American defendant used telephone and modem to download child pornography from a computer in Mexico in 1994, when the Internet was not pervasive. In R. v. Treleaven (Provincial Court of Alberta, 2006 ABPC 99, No. 060138286P1, 24 April 2006), the accused possessed 20 gigabytes of child pornography files which were identified depicted real children of both genders. While the police arrested him, his computer was still online, with dozens of other users queuing up to access the pornography.

pornography, prostitution or trading in prohibited drugs, it become a cyber casino, a cyber brothel, a cyber museum or a cyber storehouse.

Definitely, the Internet cannot be a real place for prostitution, but it facilitates the provision of and spread of information about prostitution to unspecified third parties. The Internet can also be a convenient marketplace for pirated software, books, pictures and audio discs and videodiscs. People also transact prohibited articles as well as prescribed medicine, including weapons, drugs, and philtres. Advertisements for the transaction of human organs also appear on the Internet (Li 2003).

In some countries, it is prohibited to create, replicate and spread pornography, either adult or child, either online or offline. In addition, downloading and browsing pornographic web pages is illegal as well. In some other countries, however, adult pornography is legal. The conflict of jurisdiction may also take place in gambling and prostitution, drug trafficking, money laundering, and trade in weapons and even human trafficking. It is beyond the reach of domestic laws. More than ever before, the conflicts of criminal jurisdictions have become a serious concern. Thus in the face of the Internet, state control is diminished and criminals can launch attacks from another country where law enforcement is absent.

Furthermore, the Internet is likely to become the battlefield where cyber warfare takes place. The cyber-war criminals should be held liable for offences comparable to those punished by present international criminal law.

Offences in which information systems appear as crime scenes roughly cover:

1. Intellectual property infringement,[74]

2. Collection and exhibition of child pornography,[75]

3. Sale of illegal articles (such as fire arms, alcohol, prescriptive drugs and other controlled substances),[76]

4. Online (illegal) gambling,

5. Fraud on the Internet (such as Internet auction fraud, multi-level marketing fraud).

3.1.6 Information systems as means

Computers and networks can also be a means in offences such as assault, threat, harassment, creating a false alarm, spam and fraud through text, audio or video information. Information systems are used as a means of communications in these cases. The comparable traditional mechanism is the

---

[74] Convention on Cybercrime, Article 10 criminalizes offences related to infringements of copyright and related rights.

[75] The hard drive and other deposit media can easily save thousands of images. In R. v. Paton (2005 NUCJ 7), the accused saved approximately two thousand images of children in the hard drive of his computer. In United States v. Long (Seventh Circuit No. 04-1721, 22 February 2005), the accused saved tens of thousands of images of child pornography on a computer that he kept at work (p. 1); while in the United Stated v. Newson (Seventh Circuit No. 03-3366, 5 April 2004), the perpetrator saved child pornography (pictures of his daughter and his ex-girlfriend's daughter) in his own computer. In R. v. Reynolds & Ors ([2007] EWCA Crim 538 (08 March 2007)), the police found in the computer equipment a total of "1,757 still photographs and eight movies at level 1; 1404 stills and 46 movies at level 2; 54 stills and 2 movies at level 3; 22 stills and one movie at level 4; and 7 stills at level 5."

[76] For example, in R. v. Hamilton, 2005 SCC 47, Docket: 30021, over the Internet the accused sold a package of 200 files, about 5 of which "contained material relating to constructing bombs, breaking and entering, and 'visa hacking'," one of which "contained information on a credit-card number generator" (paragraph 2).

postal system and telephone system. Dissidents have found ways of using e-mail and WWW as both media and means to air effectively their political grievances. As to information systems as a means, the e-mail and WWW simply play the function of a post office or a telephone company. Information can be exported from one part of the globe, where it is not necessarily illegal, to a state where possession of such data is criminalized. The e-mail and WWW also provide dissidents with an uncontrollable means of communication between their domestic and overseas comrades. This has implications for the freedom speech of citizens and the state stability of related countries.

Offences in which information systems act as a means roughly cover:

1. Electronic extortion, harassment, creating a false alarm, threatening, and assault,[77]

2. E-mail spoofing (phishing).[78]

---

[77] In United States v. Ray (Eighth Circuit, No. 05-1655, 15 November 2005), the perpetrator sent e-mails to a company to extort 2.5 million US dollars by threatening to exploiting a breach in its computer security (p. 1). In R. v. Lefave (Ontorio Supreme Court of Justice Court File No. CrimJ(P)6527/02, 3 October 2003), during an Internet chat between a woman and a man, the man who later became the accused stated that he "wanted to rape his seven year old daughter and kill himself." The woman disclosed the concerns to the police. He was charged with communicating a threat using a computer.

[78] Phishing "consists of creating fictitious domain names and websites all with a view to extracting bank account details from gullible individuals." See Novus Credit Services Inc v Discover Financial Services LL C [2006] DRS 03205 (27 January 2006). Through phishing site, the perpetrator can obtain "key personal details from users of the webpages to which those domain names resolved" "fraudulently" (See Alliance & Leicester PLC v Brawn [2006] DRS 4135 (18 December 2006)) or the perpetrator may acquire "confidential financial information inappropriately" (See Royal Bank of Scotland Group PLC v Laverio [2006] DRS 3953 (16 October 2006)). In United States v. Desir (Western District of Pennsylvania, 2005), the accused devised a scheme to defraud through fraudulent web sites, persons who believed they were dealing with web sites of legitimate institutions, and online auction and payment services. E-mail spoofing can also be used in e-mail bombing. For example, in United States v. Carlson (Third Circuit No. 05-3562, 12 December 2006), the accused launched two types of e-mail attacks: direct attack, in which he directly sent thousands of e-mails from different

3.1.7 Information systems used in preparation for other offences

Information systems are increasingly being used to prepare for further offences. These offences include both cybercrimes and traditional offences. More and more traditional offences against person or property seek assistance from information systems. Wasik (1991) stated that "it is certainly conceivable that a computer may be used as the means of bringing about a person's death or causing physical injury," with associated offences including destruction and damage, denial of access to authorized users, death, physical injury, and endangerment, blackmail, corruption, official secrets, etc. (p. 150) Perpetrators frequently exploit information systems in two ways. One is that perpetrators conspire through the Internet (for example Guo and Wang, Great River Newspaper, 29 July 2003). Other cases have also involved conspiracy to commit robbery, abduction, and so forth. The second manner of exploitation is that the perpetrators pursue victims through the Internet. The most common cases involve robbery, abduction, murder, blackmail, and rape (for example, Geng, Pingliang Daily, 27 February 2003).

Cybercrime is a topic covering a very wide scope. Almost all the traditional crimes, including murder and arson, can be committed with the assistance of computers and networks. To call these crimes cybercrime is not inappropriate, and consideration of the use of computers and networks into research of these

---

addresses to one address to flood it; and indirect attack, in which he sent one e-mail from one address to thousands of different addresses, but the sending address was the one that he spoofed.

crimes is also necessary.

However, this book studies cybercrimes with unique characteristics, specifically, the crimes relating to security, including the security of information systems, the security of e-commerce, and the security in which information systems serve a critical infrastructure. Although murder and arson are also tied up the issue of security, for example, the security of life and health, public security, property security and so forth, they are neither unique to the information society nor do they have special features. The crimes discussed in this book are limited to those in which information systems play a unique role, as either target, tool, route, place, medium, means, or they are used in preparation for other crimes. Other crimes may be referred to when necessary in discussing these crimes.

Offences in which information systems are used in preparation for other crimes cover a broad range, but the most usual ones roughly cover:

1. Communications in furtherance of criminal activity or criminal conspiracy,[79]

---

[79] In R. v. Poon and Wong, 2006 BCSC 1824, Docket: 23635, four offenders abducted a victim from whose family they requested a ransom, during which they sent proof-of-life photographs through the emails to the victim's family or friends (paragraph 15). In R. v. Kwok, 2007 CanLII 2942 (ON S.C.), Docket: P134/06, from the computer of the accused were revealed of about 2000 images and 60 video clips of child pornography. Along with these materials was recovered written material of "graphic chatroom conversations between paedophiles about how much they enjoy sexually abusing young children and babies and about where pictures and videos of such activity can be obtained." (paragraph 1). In R. v. O'Brien (2002 YKTC 94, Docket: 02-00176A • 02-00305), the accused used pagers, cell phones and computer internet email to communicate with cocaine suppliers and other associates(paragraph 4). In R. v. Brown, 2006 CanLII 12302 (ON S.C.), Docket: C44863, the accused used e-mail and other online communications to contact a girl on the age of 13, with the intent making her leave her family. In United States v. Christopher Lee Adjani; Jana Reinhold (No. 05-50092 D. C. No. CR-04-00199-TJH-01 OPINION, 13 January 2006), the accused were charged with conspiring to commit extortion and transmitting

2. Electronic money laundering,

3. Online tax evasion,

4. E-mail spoofing (phishing).

5. Child exploitation.[80]

3.1.8 Conclusion

It is worth noting when the potential roles of information systems in cybercrime or other crimes were classified, they were not regarded as separate ones. As it has already been noted that, these roles can possibly be separated, found to be overlapping, or integrated in one and the same case. For instance, in McKinnon v USA & Anor,[81] the accused used his own computer to access illegally 97 computers of the U. S. government, installing remote control

---

threatening communications with intent to extort, based partly on the incriminating e-mails seized in their computers (p. 7581). In R. v. Taylor and Burin ([1997] EWCA Crim 1074 (2 May 1997)), Burin made checks on the Police National Computer to obtain the address of the owner of a car (usually one he had recently sold to the new owner) and passed the information to Taylor to use it to steal the car. Burin also modified information so that stolen vehicles would appear to be recovered, enabling Taylor to possess stolen cars. In the U. K., Section 58(1) and (2) of the Terrorism Act 2000 provides that possession of a computer file of a particular nature is likely to be punished, even if it is freely downloaded from the Internet:

"(1) A person commits an offence if –

(a) he collects or makes a record of information of a kind likely to be useful to a person committing or preparing an act of terrorism, or

(b) he possesses a document or record containing information of that kind.

(2) In this section "record" includes a photographic or electronic record." Some cases have been punished according to this act, for example, R. v. Boutrab ([2005] NICC 36 (24 November 2005)).

80 For example, in United States v. Meek (No. 03-10042, 12 January 2004), the accused used the instant messenger to lure a child into a sexual encounter.

81 [2007] EWHC 762 (Admin) (03 April 2007).

software, acquiring IDs and passwords, and deleting data from these computers. He even left a message expressing his interest in hacking these computers. Here, his own computer is a tool, the Internet is a route, and the U. S. governmental computers and the data in them are targets, and so forth. In R. v. DO,[82] the accused took the minor female victims to the computer and behaved indecently while chatting online with women, during which he also touched the victims inappropriately on the breasts and vagina, showing them online pornography.[83] The roles of information systems in such cases are multiple.

In drafting legislation, it is also hard to give a clear-cut division between the different roles of information systems or of the part of it relevant in detailed offences. If any efforts are to be made for determining such a borderline, for example, one of the most puzzling situations will be met with in an offence relating to cybercriminal devices, particularly unauthorized possession, transaction, transmission, and utilization of passwords.[84] The passwords can be regarded both as a target, being a part of information systems, and a tool, for illegal access to the other part of information systems, in the same offence.

3.2 Comparison with other conceptions

After reviewing previous definitions and providing a role-oriented definition,

---

82 [2006] NICA 7 (10 March 2006).
83 ibid., paragraph 9.
84 Such conducts are criminalized in the Convention on Cybercrime as Misuse of Devices (Article 6).

the current section will turn to clarify some relevant conceptions that are usually used to describe the characteristics of cybercrime. The definition of cybercrime has long been a pending question with regard to the existing criminological theories. The alternatives have been abundant and there have been a controversial exploiting of different theories by different researchers with different standpoints or with different empirical proofs. The concepts involved in this field include white-collar crime and economic crime, etc. The following paragraphs are designed to clarify the relationship between cybercrime and some of these concepts separately.

3.2.1 White-collar crime

Unlike most other criminal phenomena that bear traditional names, the conception of white-collar crime was coined by Edwin H. Sutherland in 1939[85] and defined "approximately as a crime committed by a person of respectability and high social status in the course of his occupation" (Sutherland 1949, p. 9). The historical development of and theoretical disputes over the patterns of white-collar crime have created many different definitions (Friedrichs 1996, pp. 2-11). Yet many are still making efforts to express their new understanding

[85] Geis and Goff stated in an introduction to the 1983 version of Sutherland's book "White-Collar Crime" that "The thirty-fourth annual meeting of the American Sociological Society –convened in Philadelphia in 1939 during the academic recess between Christmas and New Year- was held jointly with the fifty-second gathering of the American Economic Association…Sutherland's talk was entitled 'the While Collar Criminal,' and it altered the study of crime throughout the world in fundamental ways by focusing attention upon a form of lawbreaking that had previously been ignored by criminological scholars." (p. ix) Therefore, Sutherland initially coined the term "white-collar crime" in 1939, published the paper in 1940, and published the book in 1949.

about the phenomenon (ibid., pp. 6-7; Helmkamp, Ball, and Townsend, 1996). The theories involved differ in emphasizing certain characteristics of white-collar crime such as "commission in a legitimate occupational context, respectable social status of perpetrators, presence of calculation and rationality (with economic gain or occupational success a primary goal), absence of direct violence, offenders' noncriminal self-image, deterrence of and, a limited criminal justice system response." (Friedrichs 1996, p. 6, citing different sources) Debates among criminologists also extend to the terminology, definition, and other issues (ibid., pp. 6-7).

The proposal for a concept "white-collar crime" was prior to the invention of the computer and the establishment of computer networks in the present sense, and most certainly before the emergence of computer criminal phenomena. The involvement of information systems in white-collar criminal activities leads people to attribute computer crime to white-collar crime because the process of the former has usually been considered impossible without a high level of knowledge or without convenient opportunities for access to the machine. The general public used to view computer crime as complicated because they had little chance for revealing the truth of the digitalized processing. In addition, the reality of computer crime has possibly been distorted due to overemphasizing business victims and underemphasizing consumer victims (Kling 1980, p. 14).

Some studies have found that cybercrime is a low-technological crime, and not a high-tech crime (Molnar 1987). With the popular use of computers and networks, more than 17 percent of the world population are connected online (Internetworldstats.com 2007), and the growth rate is still high. The tools

available to only a small group of computer users in the past are now available to a large population who have their own computers and who are connected to global networks. More and more potential cybercriminals do not need sophisticated skills for creating malicious codes by themselves. Compared with traditional violent crimes, a majority of current cybercriminals are not manufacturing guns and powder, but picking them up and shooting. Even the rest of the cybercriminals can use available programmes to produce malicious programmes to reach their goals. Therefore, "respectability and high social status" are irrelevant among today's cybercriminals.

Definitions of almost all derivatives have insisted that the offences involved are committed in the course of employment. In cybercrime, such offenders would express themselves in the form of launching inside attacks. But otherwise, I have found that insiders only make up one fifth of the cybercriminals successfully prosecuted (Li 2008a). That is to say, most of these cybercriminals do not commit cybercrime in their employment. This provides further negative proofs against the claim that cybercrime is wholly coincident with the concept of white-collar crime.

Criminal phenomena, particularly those in new fields, are continuing to be transformed from simple to complex, from more traditional to more modern, from non-occupational to more occupational. White-collar criminals' increasing exploitation of information systems is a predictable tendency.

3.2.2 Economic crime

There has never been a widely accepted definition of economic crime. An example of one definition can be taken from Sjögren and Skogh (2004, p. 1), who have defined economic crime as a crime committed to gain profit within an otherwise legal business. Recommendation No. R (81) 12 of the Council of Europe's Committee of Ministers of 1981 listed a broad range of offences into economic crime, including computer crime, particularly theft of data, violation of secrets, and manipulation of computerized data. The relevant literature has taken it as natural that computer crime is a crime in which the computer is used as an instrument of economic crime (for example, Johnson 2006, p. 1). Actually, the motives of cybercrime can be very wide and cover dozens of different kinds of crime. Profit gaining is only one of the numerous motives of cybercrimes.

Although it is difficult to find a motive behind a cybercrime (Philip 2002, p. 7), many different studies and research have drawn diversified conclusions on the classification of motives. According to Jordan and Taylor (1998), there are six common attitudes among hackers: addiction, curiosity, thrill of information searches, ability to access, peer recognition, and identifying security loopholes. Maiwald (2003, pp. 36-38) has concluded that hacker motivations fall into three categories, including the quest for challenge, greed, and malicious intent or vandalism. Kiger and co-workers (2004) have summarized the motivations of cybercrime as money, entertainment, ego, cause, entrance to social groups, and status. Pipkin (2002, pp. 17-28) has proposed that hackers may hack from a sense of intellectual motivation, such as educational experimentation, harmless fun, as a wake-up call; personally motivated, such as disgruntled employees, cyber-stalking; socially motivated, such as cyber-activism; politically motivated, such as cyber terrorism, cyber-warfare; financially motivated; and motivated by

ego. Kremen (1998) has classified hackers into ten types with "different sizes, flavours and colours."

In fact, the motives of cybercrime may vary in a way that is beyond the imagination. If we say that many cybercriminals have similar motives, we can also say that nearly every perpetrator has his or her own. Bequai (1983, pp 44-45) has summarized 17 different kinds of motives that propel the potential perpetrators to take the risk of committing computer crime. In this book, more than twenty kinds of the commonest motivations are identified and discussed according to the literature, cases and empirical studies.

The reasonable conclusion drawn from the above studies is that the conceptions of cybercrime and economic crime are correlated but not identical. Some cybercrimes can be classified into economic crime, while some others cannot. It is also clear that economic crime committed with the computer and on computer networks make up only a part of the whole phenomenon of economic crime.

3.2.3 Corporate crime

Yeager and Clinard (2006) have defined corporate crime as "any act committed by corporations, that is punished by the state, regardless of whether it is punished under administrative, civil, or criminal law" (p. 16) and they have regarded it as a particular type of white-collar crime (p. 17). It is possible for corporations to commit cybercrime, and the relationships between these conceptions are become ever more puzzling.

What is still unclear is the extent to which computer crimes are committed by corporations. In Li (2008a), corporate perpetrator was involved in only one out of 115 cases, while all other cases were committed by either a single individual or group of individuals, at most the organized groups. Although the finding of the study cannot be regarded as having universality, it has sense in that not all cybercrime are being committed by corporations or organizations (Ibid).

3.2.4 Professional crime

Insiders and outsiders constitute different ratios in different categories of offences. The categories in which the insiders constitute the majority of offenders include: data theft, espionage, and fraud (Li 2008a).

The categories in which outsiders constitute a majority of offenders include: all identity theft, 92.9 percent of embezzlement and corruption cases, 87 percent of attack and sabotage cases, 81.8 percent of viruses, worms, spyware and logic bombs, and 76.2 percent of hacking and sabotage cases. In fact, outsiders also constitute a strong ratio among fraudsters: about 42.9 percent (Ibid).

Former employees are included in the category of outsiders. A significant ratio of offenders who attack and sabotage are former employees, who constitute about 43.5 percent. Former employees also constitute 12.7 percent of offenders in hacking and illegal access cases, and about 7.2 percent of offenders in embezzlement and corruption cases (ibid).

Overall, insiders and outsiders constitute 21 percent and 79 percent of all reported offenders separately classified. Former employees constitute 16 percent of all the outsiders. If we add up former employees into insiders, they would constitute about 34 percent of the total number of offenders, still a smaller ratio than the outsiders. The safe conclusion is that cybercrime is again not a professional or occupational crime (ibid).

3.2.5 Trans-national crime

Globalization is the hallmark of modern economic and legal activities. The trans-border movement of personnel, goods, and information paints an embarrassing picture of national boundaries. Information systems alone are no longer subject to the physical limit of traditional countries. Many offences traditionally committed in neighbourhoods, communities, and native areas now extend beyond national boundaries. Many other offences traditionally committed in a trans-border manner are becoming a means to acquire new markets in the more networked globe. Some new offences can, indeed, only be completed in a trans-national style. Trans-national crime can be seen as the counterpart of international trade in civil society, being an involuntary transaction between perpetrators and the social order (in many cases, involving victims, but in many other cases, victimless).

For example, in McKinnon v USA & Anor,[86] the accused used his own computer in London and obtained unauthorized access to dozens of

[86] [2007] EWHC 762 (Admin) (03 April 2007).

governmental computers of the U. S., from which he discovered the identities of certain administrative accounts and associated passwords. He installed remote control software on these administrative computers. The software enabled him to access and change data at any time.

Many people have taken it for granted that because computer networks are trans-national, naturally most crimes committed in relation to the networks are also trans-national. This poses a great concern among academia, law-enforcement agency, and legislature. However, this is still an unanswered question. In Li (2008a), altogether 14 out of 115 cases were committed by international perpetrators or foreigners, a ratio weaker than 12.2 percent. Domestic perpetrators were responsible for the remaining 87.8 percent of cyber criminals. The majority of the reported cases are domestic computer offences (Ibid).

We can explain this phenomenon by listing the possibilities:

First, information systems have crossed the national boundaries, but prosecuted offences are mostly confined within these boundaries;

Second, due to lack of an international arrangement of law and enforcement, few trans-national cybercrime offenders have been investigated; and

Third, offences are mostly territory-dependent, and do not cross the border at all.

All these factors are responsible for the low likelihood of trans-national cybercrime, but, as we have seen and will see further, the absence of international legal harmonization and assistance mechanisms contributes primarily to the current invisibility of trans-national cybercrime.

3.3 Conclusion

The phenomenon of cybercrime is comprised of complicated acts and facts, which are multifarious, concealed and changing. There is no ready-made theory applicable for defining and categorizing various practical cases. A great many disputes exist among experts as to what exactly constitutes a cybercrime, for there is a lack of an internationally recognized criterion. Due to the lack of unified definition and classification schedule, the co-existence of different viewpoints inevitably results in conflicts in international law enforcement and to a waste of judicial resources. Cybercrime includes both new crime utilizing computer systems and new forms of existing crimes exploiting computer systems.

Theoretical and legislative classifications group cybercrimes into different categories. However, the most characteristic pattern of cybercrime is that the detailed offences are more or less linked to information systems. The roles of information systems in the offences perpetrated have the potential to develop. The starting-point of cybercrime research should focus on the recognition of the roles of information systems in the offences perpetrated. It is the information system that makes perpetrators breach security protection, to exploit the function of this system, to transmit illegal materials through this system, to operate illegal commercial activities in this system, to air offensive speech in the forum of this system, to communicate with this system, and to use this system to prepare murder, harassment and other traditional offences.

The definition does not determine the existence of cybercrime. Nevertheless, the definition endows this phenomenon a place on the academic terrain. Through definition, we are changing "cybercrime" into a research topic. Potential cyber warriors and cybercriminals may also learn from cybercrime incidences, about how they are committed, why they are reported, and what legal results are induced, etc., so that they can better trick the cybersecurity management, the victims and law-enforcement agencies. In contrast to the incentives of the crime perpetrators, scholars should analyse how and why these criminals are motivated, how and why victims are exposed, and how and why guardianships are absent.

CHAPTER 4 SUBJECTS AND SUBJECTIVE ASPECTS OF CYBERCRIME

4.1 Introduction

The motivated criminal is one of a causal trinity (together with the potential victims and weak guardianship) that produces crimes (Cohen and Felson, 1979). In cybercrime, this is also a perceivable reality. While we consider that the three factors are intertwined together, we will dedicate this chapter particularly to depicting cybercriminals and their motives.

One of this study's primary aims is to present a panorama of the cybercriminal phenomenon necessary for the establishment of a positive argument for an innovative legal framework. It is crucial to answer the questions of "who are more likely to commit cybercrime," and "what factors are more likely to motivate the cybercriminals to take the risk?" Studies and research on the subject of computer crime has had a history of several decades. Previous studies have drawn clear and steady conclusions that there was no single profile of the characteristics of a "typical" computer criminal, and that many whose characteristics meet the profile are not criminals at all (Ware, Pfleeger and Pfleeger 2002, p. 20). However, some profiles are built on empirical studies. The

earlier studies tended to "portray them as young, educated, technically competent, and usually aggressive," as Bequai (1978, p. 4) stated. Donn B. Parker (1976, p. 45) has presented a brilliant portrait of computer crime perpetrators, stating that they were typically "bright, eager, highly motivated, courageous, adventuresome, and qualified," which were the just characteristics that qualify them to employment in data processing.

The development of computer technology has changed the depiction completely (Becker 1981, pp. 18-20). There are different views about the computer systems, implying that people can use this system to do different things, and particularly, abuse the system, or pursue other deviant behaviours under the cover of technological challenge (ibid., pp. 18-20). Bequai (1983, pp. 47-50) found that while the potential sources of computer attack may vary from each other, they can, however, be grouped into three categories: dishonest insiders, outsiders, and users. This implies that everyone had an equal chance of being involved in computer crime in the age when the Internet did not expand as widely as at present. Wasik (1991, pp. 60-65) concentrated on the characteristics and classifications of perpetrators as well. Levinson (2002, p. 525) sorted out the sources of cyber threats into five groups, including insiders, hackers, virus writers, criminals groups, and terrorists. Reynolds (2003, pp. 58-65) classified perpetrators into hacker, cracker, insider, industrial spy, cybercriminal and cyber terrorist. That is to say, a broad application of computers had created a multi-dimensional social environment, and potential computer criminals had inevitably discovered the opportunities available. It is clear that the subjects of cybercrime will develop into typologies that are more and more sophisticated.

4.2 What's special with cybercriminals?

When we talk about the subjects of cybercrime, the focus is on the profile of the cybercriminal. However, the cybercriminal is not one single person, but a group of perpetrators. Many researchers have written in previous literature about "who" are most likely to commit cybercrime. Any conclusions drawn from some hundreds or thousands of cases may be premature or misleading in formulating an accurate description of a profile. More than twenty years ago, Bequai (1983, p. xviii) pointed out that the problem of the computer criminal profile can be so complex that no one single picture can be given for sketching out the panorama of this aggregation. He gave a tentative table of the profile of a typical computer perpetrator concluded from hundreds of cases in the U. S. Bureau of Justice statistics (1983, pp. 42-45). He gave the same warning against a misleading effect as many other scholars did.

As it was concluded in the last chapter, the subjects of cybercrimes can be either insiders or outsiders. Many cases have revealed that insiders constitute a great threat to their employers' systems. However, fewer younger juveniles are employed than older juveniles. That is to say, the younger juveniles may be found among the increasing number of outsiders who engage in cybercrimes. On the other hand, the nature of cybercrime is such that its perpetrators do not have an age limit. Any one who has access to computers and the Internet can act in a manner that gives rise to criminal liability.

The Internet users are strongly sex divided, that is, a higher percentage of males than females use the Internet. For example, in 2001, only 6 per cent of Internet users in the Arab States were women. It is 38 per cent in Latin America; 25 per cent in the EU; 37 per cent in China, 19 per cent in Russia, 18 per cent in Japan, 17 per cent in South Africa, and nearly 50 per cent in the U. S.[87] In Nordic countries, males have a higher percentage of daily and regular use of the Internet (Nordic Council of Ministers 2005, p. 42, Table 2.5; p. 42, Table 2.6). However, the difference is becoming smaller, with females constituting the larger group of Internet users in some countries.

This character is also transplanted into cybercriminal phenomena. According to Levinson (2002), "It is well established that boys commit far more juvenile crime, particularly violent crime, than girls." (p. 490) In fact, males have historically been responsible for the majority of overall criminal phenomena. Even in modern society, females constitute only one-third of those who commit all crimes. For example, in 2005, among the suspects investigated by the Finnish police, only 17 percent were females (Honkatukia and Savolainen 2006, p. 189). In all the offences, the highest percentage that female suspects account for are still below 30 percent (ibid., pp. 189-190). Similar patterns have also been demonstrated in many other countries.[88] Cybercrime seems less violent, but

[87] Women's Learning Partnership, December 2001. Retrieved 15 February 2016, from http://learningpartnership.org/facts/tech.phtml

[88] Take example of other Nordic countries: in Norway, females constitute less than 15.3 percent of persons charged with crimes (Norges Offisielle Statistikk. 2007. Kriminalstatistikk 2002 (Crime Statistics 2002) (NOS D 374), Table 14: Persons Charged with Crimes, by Sex and Age, p. 45); in Sweden, the percentage is about 19.7 (Sveriges Officiella Statistik. 2005. Brottsförebyggande Rådet, Tabell 200: Persons Suspected of Offences by Types of Offence, Age and Sex. Retrived 15 March 2007, from http://www.bra.se/extra/measurepoint/?module_instance=4&name=Persons suspected of offences,

research studies indicate that more males commit cybercrimes than females. In a Chinese statistical study, Jiang (2000) found that males accounted for 91.45 percent of the perpetrators, while females accounted for only 8.55 percent (pp. 151-152). He explained that the reason might be the differences between males and females in computer knowledge, skills, and attitudes to online interactions (ibid.). However, the reasons why females have been convicted of fewer cybercrimes than males are not really clear at all. The matter needs a special exploration into questions of whether females actually do commit fewer cybercrimes or whether female cybercriminals are less able to be detected. While sex is natural, gender is social. In current society, particularly in cyberspace, the boundary between (virtual) genders is vague. Thus, considerable efforts of the imagination are now being made about how genders should be defined.

Another characteristic of the subjects is that they are distributed over a broad area. Where there is Internet, there are users, and there are opportunities for abusers. Interaction and communication become more convenient, and conspiracy may take the form of online communications. Online gangs and organized crimes are capable of launching attacks from a wide range of computers. In talking about the global distribution of cybercriminals, we are not denying the global distribution of traditional criminals either. Any criminal can commit a cybercrime across territorial borders without appearing in person at the crime scene, which is a necessity in almost all the traditional offences. The cybercriminals stay where their computer hardware is located, while at the same

---

2005&url=/dynamaster/file_archive/061003/37fd76d9c15c0f2e18648590184d55cb/Persons%2520suspected%2520of%2520offences%25202005.xls); in Denmark, the figure is around 17.6 (Statistics Denmark. 2006. Statistics Yearbook 2006, Social Conditions, Health and Justice, Table 193: Convictions for Offences against the Penal Code, by Age and Sex 2004).

time their criminal activities can take place wherever information systems exist.

4.3 The perceived context of the perpetrators

The perpetrator or perpetrators behind cybercrime can vary from isolated actors to expansive criminal networks or even nation states. As stated, computer crimes can be divided into offences by insiders and offences by outsiders. Shaw, Ruby and Post (1998) classified insiders into information technology specialists such as full-time or part-time employees, contractors, consultants, or temporary workers; partners and customers with system access; and former employees retaining system access. As to whether it is insiders or outsiders who constitute the greater threat to the computer system, there have been different findings.[89] However, the mainstream findings prove that insiders have been more likely to be involved in computer crimes against the employers' systems or other abuses.[90] Insiders and outsiders also form conspirators in

---

[89] For example, The AFCOM's Data Centre Institute found that the cyber attacks launched by outsiders (52 percent) were ten times that of the insiders (5 percent). However, the respondents were more concerned the insider threats than the outsider ones. See Edward Hurley, Are Insiders Really a Bigger Threat? 17 July 2003. Retrieved 15 February 2016, from http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci906437,00.html

[90] For example, in R. v. Stanford ([2006] EWCA Crim 258 (01 February 2006)), after the perpetrator resigned from leadership of the company, he retained a 30 percent shareholding. In order to regain his position, he began to collect information to discredit the leader and force him to resign. By using the name and password of an administrator of the e-mail server, he intercepted the e-mails of the server. Another example, United States v. Pierre-Louis (Southern District of Florida No. 00-434-CR-GOLD/SIMONTON, 22 March 2002), an employee (the accused) sent a virus to his employer, and caused a two-day stoppage.

certain schemes.[91] The Nordic Council of Ministers (2005) found that students, employees and self-employed people constitute a higher percentage of Internet penetration (Nordic Council of Ministers 2005, p. 42, Table 2.5).

In addition, there is a specific category of attackers, namely, "outside insiders." They are those who were previous employees but later left the occupations. Being former employees, (some even being computer administrators), they had knowledge about the inside structure of the institution's information systems, and some even kept their accounts for access to the computers of the institution. Leaving the previous occupation, they became outsiders, but with a higher possibility than pure outsiders to misuse the institution's information systems. The reasons why they left the occupation are closely linked to their motives in the attack.[92]

The conspiracy between the insiders and the outsiders is an issue that cannot be ignored. Particularly, the co-operation between insiders and the above-mentioned outside insiders are always closely connected with an established relationship, an environment of corruption and indiscipline. In R. v. Rees,[93] a previous colleague of the accused was convicted of inappropriately

---

[91] In R. v. Jones and Singh ([1997] EWCA Crim 164 (23 January 1997)), three co-accused, who worked for the National Westminster Bank, produced screen prints of confidential information of genuine customer accounts. They passed the printouts via middlemen to the co-accused, who in turn used to forge credit cards. The forged credit cards were used to defraud from the bank of £1.2 million.

[92] For example, in United States v. Middleton (Ninth Circuit No. 99-10518, 12 September 2000), the accused dissatisfied with his job as a computer administrator in a company and quit, with extensive knowledge of its information systems. He was allowed to retain an e-mail account and used it to commit his unauthorized access and sabotage; in the United Sates v. Millot (Eighth Circuit No. 04-3962, 15 November 2005), the former system analyst of a company quit the post, but retained a Secure ID card of an account with the highest level of access possibility. With this, he repeatedly accessed the company's network and caused damage.

[93] [2000] EWCA Crim 55 (20 October 2000).

disclosing to the accused confidential information of the police, and thus inappropriately enabled the accused to have such confidential information in his possession, while the accused was convicted of aiding, abetting, counselling or procuring his colleague to do this.

Conspiracy not only happens between insiders and "outside insiders". Pure outsiders are also likely to participate in it. In R. v. Allison,[94] the accused was an insider, who acted as a credit-card analyst, having the authority to access information about the company's debtors. She got instruction on accounts that she should work on, but she could also access other accounts. Upon accessing other accounts, she provided information about them to her outside co-conspirators. With that information, one of the outsiders drew large sums of money from Automatic Teller Machines (ATM).

Mackenizie and Goldman (2000) reported that some students, particularly computer science and engineering majors, with newly discovered skills, attempted to break into the servers of the University of Delaware (p. 174). CSI reported that 55 percent of survey respondents reported malicious activity by insiders (Nelson 2004, pp. 299-321). Researchers also revealed that dissatisfied employees were a major source of computer crimes (Vatis 1999) and were the greatest threat to computer security (See Sinrod and Reilly 2000, pp. 183-187). When Sutherland suggested the term "white-collar crime" in the late 1930s, he could hardly have imagined that there would be crimes occurring in the process of human-machine-human interaction, other than the human-human interaction, human-organization interaction, or human action against the machine. Nevertheless, the term "white-collar cybercrime" or "cyber white-

---

[94] [1998] EWHC Admin 536 (13 May 1998).

collar crime" has also come into use at the present time, apparently as new development of Sutherland's theory.[95] Michalowsky (1996) explicitly attributed computer crime to white-collar crime (p. 175), because computer crime was an "insider crime" (p. 177), computer crime violated "trust" (p. 178), computer crime aimed at "personal or organizational enhancement" (p. 179), computer crime was "administratively segregated" (p. 180), and computer crime drew "limited enforcement attention" (p. 181).

In my opinion, the concept of white-collar crime cannot perfectly fit the situation of cybercrime. Yet the term "white-collar crime" emphasizes the occupation and social status of the criminals, and one of the most relevant factors in white-collar crime is the knowledge that the criminals acquire from both their pre-employment education and their occupational career. It is hardly oversimplified to view white-collar crime as a knowledge-based offence compared with violence-based traditional offences. As to the defining of cybercrime, it can be viewed either as a knowledge-based white-collar crime or as knowledge-based cyber violence. In the former case, it is white-collar crime; in the latter, it is not.

It is reasonable to conclude that, when there were few computers, employees in computer-related industries were the only computer users, and were small in number. They acquired more chances to launch attacks against their employers. With the prevalence of personal computers and the development of the Internet, insiders remain to take advantage of having better

[95] See for example, "Victim Assistance Online" Web site. Retrieved 15 February 2016, from http://www.vaonline.org/internet_wcollar.html. The term "White-collar Hacker" is also used, for example, by Leyden, J. The Rise of the White-collar Hacker, 2004. Retrieved 15 February 2016, from http://www.theregister.co.uk/2004/03/31/the_rise_of_the_white/

knowledge about access-control mechanisms, asset management systems, and overall loopholes. Insider knowledge, convenience, and directness encourage undisciplined employees to commit cybercrimes. As the U. S. Secret Service and CERT Coordinator Centre's study disclosed, minimal technical skill is required to launch cyber attacks on the banking and finance sector (Randazzo and co-workers 2004).[96]

In addition, insiders expose themselves to a negative psychological influence derived from their information work environment. Shaw, Ruby and Post (1998) identified the factors that increase the tendency towards illegitimate and harmful behaviour among employees, as including computer dependency, a history of personal and social frustrations (especially anger toward authority), ethical flexibility, a mixed sense of loyalty, entitlement, and lack of empathy.

On the other hand, offences by insiders involve a less complicated process of tracing, detecting and investigating than in the case of outsiders. If we cannot judge whether insiders or outsiders are liable to commit more cybercrimes, we should firstly consider the question of which group are more likely to do it and which group are more likely to be caught. Insiders surely coincide in both of situations: insiders commit it and they are caught. Therefore, everyone knows that insiders pose greater threats, and outsiders are exempted from reprimand. Furthermore, it is more efficient for the law enforcement to reveal an inside misuse than an outside attack, they are rationally more likely to pay more attention to the current and previous employees. Incidents involving outsiders and or international actors will more likely to be disregarded at first

[96] In different studies, the term "insider" is defined differently. In Randazzo and co-workers (2004), insider was defined as including "current, former, or contract employees of an organization."

glance.

4.4 Forms of organization

The social actors can roughly be classified into two categories, natural individual actors and corporate actors (Coleman 1990). The classification has been used to categorize criminals into individual criminals and corporate criminals, for example, Sutherland (1949), Alvesalo and Laitinen (1994, pp. 11-66), etc.

The subjects of cybercrime -in this case the perpetrators- are as complicated as those of traditional crimes. We can touch further beyond the ideal typology for a combination of individual persons. First, individual persons act independently, in which case the perpetrator should necessarily appear on the scene.

Second, individual persons act separately, but dependently, for example in cases of mobs and other collective actors, in which the actors necessarily appear on the scene, and their absence is exceptional.

Third, individual persons act together. They are dependent, interrelated, and coordinated as in the case of organized crime. They do not necessarily act physically in person. When an offence is committed, some are on the scene, while some are not, for example, the organizer of the crime. A collective presence is optional.

Fourth, individual persons act together. They are dependent, interrelated, coordinated, but not necessarily physically in person. A collective presence is

exceptional.

An individual belongs to a single non-collective class. However, the individual also belongs to the group of the non-organized class. Furthermore, the individual, group and organization belong to the same non-institutionalized class. The organization and corporation both belong to the organized class, but the corporation is further located in the institutionalized class. In addition, the criminal group and criminal organization are both criminal collectives, being illegitimately formed. The corporation is formed legitimately.

Extending the discussion a little further. The individual is directly linked to the family. Group is usually beyond one family, but is limited to the neighbourhood. Organized crime has a broader range of influence, that is, the community. These three units can play important roles in crime prevention against the individual, group, and organized crime both separately and together. A corporation is established by the authorization of the state, and the primary prevention unit should be the public sector.

As Kelly (2002) has summarized it, cybercriminals may be those who shift from traditional crime into a new world, discontented personnel, cyber adventurers, and cyber spies and cyber warriors.[97] It is reasonable to claim that these individual criminals, corporate criminals, and particularly, a criminal organization all have the tendency to extend their criminal activities into cyberspace. Sometimes even cyber mobs will act against law and order in cyberspace.

---

[97] Kelly (2002) stated that: "Perpetrators can be from the traditional criminal world exploiting the power of the new tool, disgruntled employees using their inside knowledge, the curious and thrill-seekers treating the medium as a challenge and those engaged in industrial espionage and information warfare."

In the case of natural persons, the social status, age, and education background of computer criminals cover a broad range. They may be "students, amateurs, terrorists, and members of organized crime groups" (UNCJIN 1999, Paragraph 32); or people with varied skills, knowledge, resources, authority, and motives (Parker 1998); and people with different levels of skill in formal education, social interactions and use of computer systems (Parker 1998). Particularly, virus writers also "vary in age, income level, location, social or peer interaction, educational level, likes, dislikes and manner of communication." (Kabay 2001)

If we say that cybercrimes by individuals have already run rampant, organized cybercrime, cyber terrorism, and cyber laundering will be even greater emerging threats to the networked information society.

The 9/11 attacks on the U. S. raised great concern about organized cybercrimes, cyber terrorism and cyber laundering. Although many commentators have made efforts to define organized crime, Feldman (1993) has identified three key features of such organizations: making money as the goal; corrupting the police and public officials; and being a family business (p. 16). In this sense, no organized cybercrime has ever been reported in real life. Although organized cybercrime can be regarded as falling within the domain of actions of natural individual criminals, it has such particular properties that it deserves a special inquiry.

Information systems have dual roles, being a critical infrastructure of society and potential targets for crimes; and being the means as the communications system and being the route that facilitates electronic-money laundering. A growing concern is that the organized crimes and cybercrimes are

increasingly interwoven. Bequai (1979b, p. 201) stated: “Organized crime now operates with impunity and the knowledge that it enjoys de facto immunity from prosecution.” The computer systems is infiltrated by organized crime (Bequai 1983, pp. 55-69), becoming its tools to operate drug trafficking, gambling, loan sharking, theft of cargo, prostitution and bootlegging of cigarettes, labour racketeering, coercive practices, and economic crime (p. 59). Everything that traditional organized crime has been doing can now possibly be done with the help of information systems, which play different roles in offences.

The ways in which international organized criminals exploit information systems, including making obstacles by technical means to escape official investigations, raising funds through cyber offences, using online services in money laundering, publishing online advertisements, and realizing trans-border money laundering through electronic banking and commerce systems (Lilley 2003, p. 117). Williams (2001) identified that criminal groups are using the Internet in property crimes, white-collar crime, and money laundering, and the organized crime groups that use the Internet for communications and for any other useful and profitable purposes.

Most cybercrimes are not necessarily organized; however, organized forms of cybercrimes have greater threats than unorganized forms. Organized crime simply means a crime that is committed by organized perpetrators. In the case of cybercrime, there are some forms of offences like organized crime, but in practice, they are merely individual crimes. For example, distributed denial of service attacks are launched from compromised computers distributed in different locations. These computers can be “organized” by one or more

persons. However, the crime in which "organized" computers are used as tools does not necessarily form an organized crime.

The U. S. Department of Justice (2002) reported an organized software piracy case. According to the report, the DrinkOrDie online software piracy group was specialized in acquiring and cracking new software and releasing cracked software over the Internet. The leader and about 65 members from more than 12 countries in the group adopted a hierarchical organizational structure, grouping members according to their different functions (U. S. Department of Justice, Press Release, 17 May 2002).

In considering the problem of organized crime, the UN Convention against Trans-national Organized Crime should not be ignored. The Convention defines organized criminal groups as "a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit."[98] For how long a period of time the group exists has not been clarified in the Convention, while serious crime means a crime punishable by at least four years of imprisonment.

Although there is increasing concern on cyber terrorism, the understanding of what cyber terrorism constitutes is unclear. Generally, it is a concept that is comparable to traditional terrorism. Many characteristics can be induced from the concept "terrorism"; however, the most significant factors may be political motivation, violent effect and fear creation. The following two

[98] The UN Convention against Transnational Organized Crime (A55/383, 2000), Article 2.

definitions prove that these respects are also critical in identifying "cyber terrorism". The FBI's definition of cyber terrorism has emphasized the political motivation and the violent effect in an attack on information systems:

"The premeditated, politically motivated attack against information, computer systems, computer programmes, and data which result in violence against non-combatant targets by sub-national groups or clandestine agents." (Pollitt 1997, Cited in Robert 2004, p. 124.)

The U. S. National Infrastructure Protection Centre's definition has focused more on the fearful effect of such an action, among many other harms:

"A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social or ideological agenda." (Garrison and Grand 2001, p. 2)

As Weimann (2004, p. 6) claimed cyber terrorism becomes an attractive choice for contemporary terrorists for several reasons. It is cheaper, more anonymous, aiming at a more enormous target and number of targets, remotely conducted, and affecting a larger number of people worldwide. International society has hardly implemented any countermeasures against traditional terrorism in the last few years. At present, further actions should be taken to respond to the rising threat of cyber terrorism. However, from lack of practical cases, cyber terrorism remains a theoretical assumption and a supposed or partial threat. Scholars, politicians and mass media tend to connect terrorists with information systems, but these efforts appear feeble since the fact that the

terrorists are still able to utilize the traditional post, transportation, and courier. As Harvey (Financial Times, 3 December 2003) pointed out, cyber terrorism remains an unimportant matter.[99]

Theorists of the early 2000s overemphasized the problem of cyber terrorism for several reasons: Firstly, the panic caused by the previous century's Asian financial crisis continued in the uncertain new century. Secondly, the denial of service attacks against web sites during this period seemed to portend the possibility of the collapse of information systems and the information economy. Thirdly, for the mainstream American theorists and law enforcers, the 9/11 attacks on the U. S. were interpreted as a strange hint that cyber terrorism could also cause similar casualties in which thousands of people lose their lives. Fourthly, eschatological ideas still dominated the brains of most people in considering that the end of the world may be expressed in the form of end of the society, in particular, the information society.

The research on cyber terrorism is primarily for the purpose for raising the awareness and preparedness of the authorities (because once occurring, cyber terrorism should be dealt with at the first moment by the authorities), the legislature, politicians (because it is politically motivated) and the general public (because it is assumed that the general public are the most frequent victims, even if the attack is targeted at a certain person, building, vehicle, or certain part of information systems).

---

[99] The present wars on real world terrorism being continued, critics revealed that the wars are based on "selfish" politicians' distortion and exaggeration of the threats posed by terrorism. See Stewart Nushbaumer, The Abuses of 9/11, 2002. Retrieved 15 February 2016, from http://www.911digitalarchive.org/collections/reports (saying that the wars were being exploited by the forthcoming party elections); DeBose (2004); O'Brien (2004) (saying that the so called war on terrorism included "inexcusable misrepresentation").

4.5 Age and cybercrime

A noteworthy phenomenon is that, regardless of individual cybercrimes, or corporate cybercrime, young perpetrators play a critical part. Although there is no age limit for committing the cybercrime, as there is for traditional crimes, young people constitute an important part of the cybercriminals. As Shannon (1993, p. 2) reported, cybercriminals usually tend to be between the ages of 14-30, they are usually bright, eager, highly motivated, adventuresome, and willing to accept technical challenges. The age of criminal responsibility is prescribed differently between various countries. In most countries, children under 14 or 15 years of age are not liable for a criminal offence, while children between 15-17 or 14-16 years of age are liable for a limited range of offences.[100] In fact, juveniles commit a number of these crimes. In China, people between the ages of 19-40 constitute 80 percent of the Internet users, and the average age of the cybercrime perpetrators is 23 years old (Dong 2003). Juvenile delinquency and juvenile justice became issues closely associated with cybercrime. According to Howitt (2002), the reason why children are more likely to commit crime is not that more and more children will commit crime, but that most of the potential offenders will commence to commit crime in childhood and continue their criminality for much of their lifetime. After 16-17 years of age, the offending

[100] For example, in China Penal law, children under 14 years old of age are not liable; in Finish Penal law, the age limit is 15. In some other countries, the age of criminal responsibility is even lower. In England and Wales, the age is 10 years, while the there is a partial criminal responsibility between 10-14 years of age.

rates decreases to a plateau (pp. 76-77). Through empirical studies, the following reasons show why juveniles have a greater tendency to commit more cybercrimes:

(1) People of different age groups use computers and networks in a different environment. Adults usually use computers and the Internet at work. When they go home after work, they have to do housework, take care of children, or are engaged in sports and recreation. The youths, including young couples without a child, use computers and the Internet at any time, and for a long time everyday. For example, about 57.9 percent of the Internet users are unmarried (China National Networks Information Centre, Statistical Survey on the Internet Development in China 2006, pp. 14-15). Many of them are not employed. In addition, some of the employed also use computers and Internet for many hours in their spare time. Students and employees in enterprises constitute 64.8 percent of the Internet users (ibid., p. 16). Youths use computers and the Internet for purposes of education, communication and recreation. Chatting and gaming are the commonest forms of online activities. Offline dating with online mates has become popular. Of the 111 million Chinese Internet users in January 2006, about 16.6 percent are under the age of 18, about 35.1 percent are between 18 and 24, about 19.3 percent between 25-30, about 11.6 percent between 31-35, about 7.1 percent between 36-40. Users older than 41 account for only a little more than 10 percent (ibid., pp 12-13). The U. S. Census Bureau surveyed households with computers and Internet access by householder age. The findings indicate that the 35-44 and 45-54 age groups have the highest penetration, more than seventy per cent own a computer and over sixty-five percent had Internet access. The survey found

that the critical factor in determining whether a household had a computer or Internet access was the presence of a school-age child.[101]

A similar characteristic has also been found in Finland where one parent or two parents with children have access to the Internet at home with a higher percentage (Nordic Council of Ministers 2005, p. 39, Table 2.2). In all of the Nordic countries, the age groups of 25-34, 16-24, 35-44, and 45-54 have the higher penetration percentage (ibid.). This increases the opportunities for harming others and the probabilities of being victimized.

(2) People of different age groups have different interests in using computers and networks. The adults devote themselves more to profession and family, apart from the fact that their energy and interests are more concentrated on issues of greater concern. Youths are neophiliacs, with sharper curiosity and passion for an unknown field, and more hobbies. According to the Nordic Council of Ministers (2005), with an increase in age, the use purposes of the Internet declines. Youths use the Internet in noticeably more varied ways than elderly people do. Sixty percent of people under 30 years of age and exactly 14 percent of people from 60 to 74 years of age find at least eight purposes to use it (Nordic Council of Ministers 2005, p. 36). The Mentor, the author of "the Hacker Manifesto" confessed that: "Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me..."[102] The youths are also prone to addict themselves to computers, the Internet, and virtual reality. The Mentor described that:

"And then it happened... a door opened to a world... rushing through the

---

[101] U. S. Census Bureau, Computer and Internet Use in the United States: 2003, published in 2005.

[102] The Mentor, The Hacker Manifesto, 8 January 1986.

phone line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetence is sought... a board is found."[103]

The share of virtual life in their daily life is increasing, at the share of real life decreases. To the extent the youths spend more time in cyberspace, the bigger the probability is that they involve themselves in online illegal activities (besides legal ones).

(3) People of different age groups have different structures of knowledge, techniques and skills on computers and networks. The adults generally grasp the knowledge, techniques and skills for their occupational use. This does not exclude that they were ever good at pre-Windows operation systems and interfaces, for example, MS DOS, etc. However, adults have less intention of exploring the higher techniques and skills on computers and Internet, particularly those irrelevant to their profession. The young people are motivated by their curiosity and engaged in "learning-trying". They are willing to try either useful or harmful content, programmes, messages or activities. They easily act in a way that sometimes generates a legal concern.

(4) People of different age groups have a different legal consciousness and sense of social responsibility. The adults are more socialized and have a higher level of legal consciousness and stronger sense of social responsibility. They are not willing to harass others or disturb the public. Youths are in the process of being gradually socialized, with lower level of legal consciousness and a weaker sense of social responsibility. In practice, many juvenile cybercriminals are not conscious of the nature of their harmful activities. They think more about themselves than about the public, more about process than about result, and

[103] ibid.

more about the power of technology than about the negative influence. They just do not recognize the harmfulness of their dangerous behaviour before they attract the attention of the law enforcers.

(5) People of different age groups have a different risk calculation and expectations of costs in deciding whether to carry out cybercrime. Adults who have their stable professions, families, reputation, and social status are not likely to carry out more risky and more costly activities, particularly harmful hacking. They feel they can only benefit far less from illegal activities than engaging in legal activities, and thus have less incentive to hack. If they commit this kind of act and are caught, their losses will be great and in a broad range. The possible result deters them from acting with a negative social and legal evaluation. Young people generally have a less stable social status and less to lose if they are caught for hacking. Their incentive to hack is surely bigger than adults are.

(6) People of a different age group hold different attitudes toward crime. Adults have more mature thinking about criminal phenomena. The harmfulness and risk of crime have impressed them to stop before crime at every moment. Youths are not as mature as adults are and are less capable of controlling their enthusiasm. The temporary impulsion usually results in irrecoverable activities.

(7) People of different age groups demonstrate different fluidity. The personality development of the adulthood is characterized by stability: "stability is the rule." (Smith 1998, p. 397) Adults are apparently more stable than youths in employment, families, social status, and reputation. The youths are in a situation of development and usually move from here to there. During this process, they are easy to have more spare time alone. Due to lack of acquaintances, they take part in traditional social activities less but in online

interactions more. In particular, in regions in the process of urbanization, the existence of latch-key children provides an incentive for private enterprises to operate premises for access to network services and games, these becoming largely uncontrolled places so that undisciplined children engage in unmonitored activities.

(8) People of different age groups hold different attitudes toward fortune and fate. Adults have more life experiences and social knowledge, and are more aware that criminals can escape punishment temporarily, but that mostly they will be caught and punished later. Young people have a more unreasonable imagination of being able to escape from law enforcement, particularly when computers and the Internet provide such an indirect way of carrying out a criminal scheme.

(9) Criminal-victim relations are easier to establish between online users. Because youths tend to use computers and the Internet in a more frequent way, both cybercriminals and cyber victims tend to be people inside this age group. The same rule can be applied to organizations. Although it is unfeasible to measure the age of an organization, the ages of the personnel may serve as an indicator of the online business of this organization. If a company is owned or managed by youths, it is more likely to engage in some kind of online business, and more likely to be victimized as well.

(10) Young people more easily escape arrest and punishment than adults are. This does not mean escaping in the physical sense, that is, “to run”. Rather, young people are less stable and fixed in terms of social status, and may have better chances of avoiding arrest by moving from one place to another, without further responsibility for employment or family (if they are not employed or

married).

In sum, youths may have more chances for access to computers and the Internet and are more likely to commit cybercrime. Certainty, they more easily harm others and are themselves more easily victimized.

4.6 Psychological features of cybercrime

Cybercriminals have a multiplicity of motives. The prolific functions and services of information systems create diversified incentives for their users to commit crimes. Criminals can be satisfied physically or psychologically through various online offences. As I have summarized the matter in the last chapter, cybercriminals can be motivated by a broad scope of internal driving forces. Cybercrime becomes an attractive industry for those who are seeking profitable opportunities.

The perpetrators do not have a particular sense of guilt. The absence of the traditional crime scene and the remote control of the process render things different from the traditional crime scene. Technological involvement makes the process of most cybercrimes less violent. This results in a reduction of ethical and legal responsibility and of psychic cost, and creates an incentive to start, continue and repeat the offences.

The perpetrators depend more on fluky elements. Information systems provide chances for criminals to conceal their criminal traces and make it difficult for them to be discovered. The easy escape from moral pressures and the difficult detection process lower the psychic cost and increase the psychic

sense of security. As the Hacker Manifesto stated that: "You may stop this individual, but you can't stop us all …"[104] The deterrent effect of punishment on the cybercriminals is in turn reduced. More potential perpetrators are thus encouraged to participate in unlawful online activities.

Furthermore, the Internet creates a space where people are not meeting face-to-face, but meeting mind-to-mind (Hagerty 2000, p. 181). The cyberspace facilitates a new style of interpersonal interaction that develops through the mediation of machines beyond the physical appearance of the participants. However, minds under this easy sense of falsification can only develop a vulnerable relationship and expose potential victims. E-mail frauds and viruses are a source of exploitation harvesting from the blind trust of remote recipients, enmeshed in the so-called social engineering structure. In Tektrol Limited v. International Insurance Company of Hanover Limited and Great Lakes Reinsurance (UK) Limited,[105] an attachment of an e-mail purported by a Christmas card from a trustworthy source was activated by the recipient and erased system files on the computer causing it to cease functioning, and more seriously, erased the source code that the recipient company developed.[106]

---

[104] The Mentor, The Hacker Manifesto, 8 January 1986.

[105] [2004] EWHC 2473 (Comm), No. 2003 folio 940.

[106]. The court noted that:

"The virus author had no knowledge of or connection to the Claimant or its source code. Although he did not specifically intend to erase the Claimant's source code, he intended the virus programme to spread around the world and knew that whenever the virus programme was activated by the opening of the 'Christmas card' attachment, computer data could be erased on the computer concerned."

ibid, appendix, assumed facts for the preliminary hearing, Paragraph 20.

4.7 What motivates a cybercrime?

Cybercriminal behaviour affects many scientific disciplines. In research on cybercrime, the term motivation is used in a broad sense, and is usually interchangeable with motive. Motives are nothing more of a mystery than the wants and wishes the goal-directed activities endeavour to gratify (Smith 1998, p. 422). A strict distinction cannot be made between these two words. Therefore, Maslow's "need hierarchy," which lists need in a order of priority as physiological needs, safety and security needs, belongingness and love needs, esteem needs, cognitive needs, aesthetic needs and need for self-actualization (Maslow 1954), is not consistently relevant with the analysis here. The forces behind the individuals' decisions to commit cybercrimes are different from one another. In understanding cybercriminal behaviour, we have to recognize psychic benefit in some cases and for some people. Cybercriminals can demonstrate an extensive scope of self interests. Although it is difficult to find a motive behind a cybercrime (Philip 2002), many different studies and research have drawn diversified conclusions on the classification of the motivations. According to Jordan (1998), there are six common beliefs among hackers: addiction, curiosity, thrill of information searches, ability to access, peer recognition, and identifying security loopholes. Maiwald (2003, pp. 36-38) concluded that hacker motivations could be divided into three categories, including the search for challenge, greed, and malicious intent or vandalism. Kiger and co-workers (2004) have summarized the motivations of cybercrime as money, entertainment, ego, cause, entrance to social groups, and status. Pipkin (2002, pp. 17-28) proposed that hackers may hack from an intellectual

motivation, such as educational experimentation, harmless fun, as a wake-up call; personally motivated, such as disgruntled employees, cyber-stalking; socially motivated, such as cyber-activism; politically motivated, such as cyber terrorism, cyber-warfare; financially motivated; and motivated by the ego. Kremen (1998) classified hackers into ten types, including curious hacker, thrill seeker, the person who wants information about computers and their flaws, power seeker, vandal, the person who steals industrial information, secrets and/or intellectual property, the person who steals money, the person who performs industrial espionage, terrorist, and international spy.

In fact, the motives of cybercrime vary in a way that is beyond the imagination. If we say that many cybercriminals have the similar motives, we can also say that nearly every perpetrator has his or her own. Bequai (1983, pp 44-45) has summarized 17 different kinds of motives that propel the potential perpetrators to take the risk of committing computer crime. This section will identify and discuss 29 kinds of the commonest motives, without deliberately avoiding coincidence with the different lists created by previous scholars.

(1) Pursuing information freedom

A free flow of information is a requirement for ensuring the free movement of goods, persons, services and capital.[107] In cyberspace, people who hold the view that the Internet is a public place, and thus everyone has the right of obtaining information, are not rare. Under the dominance of the hypothesis of information freedom, many information systems users take the risk of breaching others users' privacy and trade secrets. Levy (1984), Selwyn and Gorad (2001), and Himanen (2001) have shown that many traditional hackers

---

[107] Directive 95/46/EC, Preamble (3).

are motivated by a belief in the freedom of information. These hackers have insisted that all the useful information must be freely copied, distribute, studied, changed, and improved, but their ethical code prohibits destructive activities against any information.[108] What is problematic is that unauthorized access to confidential data has been criminalized, even in pre-computer times. If e-mail is comparable to a letter, and if free information advocators can freely open e-mail, a natural conclusion will be that everyone can destroy mailboxes and open letters. The only difference is that the present files exist in digital form. Access to confidential information is punished by laws penalizing offences infringing privacy, intellectual property, trade secret, and state secret. Therefore, the freedom of information is limited to information that is granted free access but access is not free to information that is limited. The other end of the free flow of information is the safeguard of the fundamental rights of individuals.[109]

(2) Achieving ego expression

Hackers also have the possibility of hacking for the sake of their ego, for proving a self that is different from the selves of others. Perpetrators in this category are usually frustrated in social competition elsewhere and seek an opportunity to compensate by employing their computer techniques. Through

---

108 See Branscomb (1990). The focus of the hacker ethic is on the freedom of information. The hacker ethic was initially created by the MIT hackers in the late 1950s to the late 1960s and articulated by Steven Levy in his book "Hackers: Heroes of the Computer Revolution." The general creed includes the following aspects: "1. Always yield the Hands-On Imperative! Access to computers-- and anything else which might teach you about the way the world works-- should be unlimited and total. 2. All information should be free. 3. Mistrust Authority-- Promote Decentralization. 4. Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position. 5. You can create art and beauty on a computer. 6. Computers can change your life for the better." See Logik Bomb, Hacker's Encyclopedia, Second Revised Edition, 1997.

109 Directive 95/46/EC, Preamble (3).

success in surrendering to information systems, they supersede others in hacking techniques and skills, even though they have an apparent inability that leave them incompetent with others in social activities generally. Yan and Zhang (Beijing Youth Daily, 6 November 2001) have reported the case where a 17-year-old hacker intruded into an official human-resources web site, defaced the homepage, formatted the hard disk of the server, and destroyed a great deal of data. It was reported that during his sick leave at home, the hacker had picked up his hacking knowledge from the hackers' web sites, and downloaded some hacking programmes. Then he found some web sites with security holes and intruded into them. At first, he sent messages to the administrators of these web sites, telling them that their web sites had loopholes. Without receiving any reply, he got angry and defaced some of these web sites (Yan and Zhang 2001).

(3) Challenging technical difficulties

Technical challenge has been long identified as a motivation. Pipkin (1997) regarded challenge as the biggest motivation, meaning that the hacker is excited after succeeding in his attack on most secure systems. In one case, a hacker created a Trojan programme named IPXSRV, and gained control of 60,000 computers. He manoeuvred this colossal "botnet"[110] to launch denial of service attack against a music web site for three months before the police detected it. Investigation revealed that the hacker had been seeking a chance to try the power of his Trojan programme, and chose this web site as a target of denial of service attack. As a result, the web site was broken down for three months (Secretchina 17 March 2005).

[110] Botnet is "a collection of compromised computers controlled by the same intruder, often [using] remote control software or Internet Relay Chat (IRC) services." Daintith (2004), p. 56.

(4) Seeking knowledge

Cybercrime motivated by a desire to seek knowledge is not rare in practice. Jordan (1998) reported the motivation of Kevin Mitnick, the most famous of all hackers was to gain knowledge, seeking a better understanding of information systems.

Many computer and Internet users are motivated to acquire knowledge from the devices, information and new space. Both hardware and software are the targets of their knowledge-seeking attempts. Hackers are seeking knowledge through access to others' computers by fair means or foul. "The Hacker Manifesto" clearly expressed the motivation behind hackers of this kind. It stated that cyberspace was a world of "the electron and the switch," and hackers were called criminals due to their use of the services without paying during their seeking after knowledge motivated by curiosity.[111]

(5) Testing system security and resilience

Technical primacy is one of the most important answers to the question "what do hackers hack for?" The common sense knowledge about the attacks is that hackers identify flaws in systems or software, to allow the developers or the administrators to fix them (See Branscomb 1990, p. 24). For example, Brian West used MS Front Page and a web browser to identify a security flaw in some web sites that allowed him to have access to proprietary information and password files (See U. S. Department of Justice, Press Release, 24 September 2001). Hacking for security may be quite the same to hacking for insecurity: on the one hand, the unauthorized intrusions into the protected systems are illegal; on the other hand, the publication of security flaws also poses a real danger for

---

[111] The Mentor, The Hacker Manifesto, 8 January 1986.

the systems.

In addition, some physical damage to information systems is also possible when testing the resilience of factors under operating conditions. For example, in R. v. Feltis,[112] one of the explanations of the accused about why he had apparently sabotaged the company's computer was that he had been testing the computer, and particularly its resilience to interference, by disconnecting two cables and reconnecting them, as a result of which an impairment of the computer was caused and an enormous disruption of the business of the company occurred.

(6) Adventuring risky online activities

Traditional adventurers have sought psychic satisfaction from conquering things others have seemed unable to do, and during which they overcame unimaginable difficulties. The modern adventurers have also found challenges in the field of technology, from telecommunications, computers to the networks. The ability to influence huge systems may be satisfying in and of itself.[113] Activities, either benign or malicious, on the "electronic frontier" involve the factor of adventure, that is to say, to explore the unknown (Grabosky 2000, pp. 2-3). What Donn B. Parker called the personification of computers (Parker 1998) is also such a motive. Sophisticated viruses indicate that writers who believe that their works contribute to the development of

---

112 [1996] EWCA Crim 776 (19th August, 1996).

113 See Ministry of Justice (1985), p. 206; Howerton (1985), p. 54; the United Nations Crime and Justice Information Network (1999), Paragraph 74; Schwartau (1994); Branscomb (1990), p. 24; Grabosky (2000). Creator of Melissa Computer Virus said that he constructed the virus to evade anti-virus software and to infect computers using the Windows 95, Windows 98 and Windows NT operating systems and the Microsoft Word 97 and Word 2000 word processing programmes. See United States v. Smith (D. NJ) 2 May 2002.

science and technology have created them (Kabay 2001).

Adventure is closely associated with the conception of curiosity. Under the drive of curiosity, considerable examples of such curious intrusions have happened, which had catastrophic effects (Howerton 1985, p. 54).

Adventure is not always a simple motive that can be explicitly identified. Sometimes, it is closely related to other motives, and in other cases, the adventure motive may be ambiguous. According to The Associate Press (19 March 1998), when the hacker, who called himself "The Analyser", and launched an attack against the Pentagon's computer systems, was identified by the U. S. Department of Justice and questioned by a special police anti-hacker unit, the chief administrator of the country from where the 18-year-old boy came praised him: "Damn good, very dangerous, too." [114] Soon after the incident, the hacker was drafted into the national army to serve in an information warfare division, an assignment which utilized his computer talents.[115]

(7) Trying programming skills

In contrast to testing hackers who try to identify flaws in computer systems, experimental hackers try to reveal the functions of hacking programmes. Whether the systems are secure or not is irrelevant. Actual intrusion into the systems is only an occasional result. Many Internet users did experiments of this kind with software downloaded from the Internet, or programmes compiled by them, and sometimes no actual intrusion succeeded. Relatively unprepared and unintended, experimental hackers are usually the "first

[114] Pentagon hacker Wins Praise, Associated Press, 19 March 1998.
[115] Israeli Teen Hacker Details Prowess, Associated Press, April 1998.

offender". Their purpose is to test the function of intrusion programmes or techniques, during which they accidentally succeed in acquiring unauthorized access to the systems.

(8) Tentative attacks

Tentative hackers are similar to experimental hackers in the way that they are unprepared intentional intruders. Nevertheless, a distinctive point is that tentative hackers try to use hacking programmes or intrusion techniques. Whether the system is secure and whether the intrusion is successful are both irrelevant considerations. For example, some users operate password-cracking programmes to access others' encrypted information. Internet users sometimes also try to guess other users' account ID and passwords so as to enter their systems.

(9) Expression of hatred

Hatred may come into being for a variety of reasons. Dissatisfied employees damage their employers' assets. Dissidents are motivated to destroy the states' critical infrastructure. The hacktivists, anarchists, and terrorists all launch attacks against targets regardless of their nature. Generally, hatred leads to attempt to weaken the counterparts' social priorities. Examples include ruining computer systems;[116] destroying information (Howerton 1985, p. 55); revealing confidential data (Grabosky 2000, pp. 2-3); and defacing abhorrent web pages (Grabosky 2000, pp. 2.-3).

Envy may also lead to hatred. In cybercrime, attackers commit sabotage

---

[116] For example, in prosecuted cases such as United States v. Garcia (C. D. Cal.) 23 February 2004; United States v. Diaz (S. D. Fla.) 5 December 2003; United States v. Patterson (W. D. Pa.) 2 December 2003; United State v. Lloyd (D. JN) 26 February 2002; United States v. Ventimiglia (M. D. FL) 20 March 2001; United States v. Sullivan (W. D. NC) 13 April 2001; United States v. McKenna (D. NH) 18 June 2001.

due to envy of others' wealth, competitors' success, and colleagues' achievements.

(10) Hacking for financial gains or avoiding payment

Not only has information itself value, but information systems are also used widely in the financial sector (Parker 1998). Because the function of the computer in accounting enables a wide use of computers in financial management, embezzlement has been made easier by numerous methods (Howerton 1985, p. 54). These methods may include information selling without the right to do so; extorting from the victimized organization; embezzling from employers; illegally obtaining information to sell to competitors; electronic theft of credit-card numbers; and stealing personal information to impersonate someone financially (Ministry of Justice 1985, p. 206).

The perpetrators steal, swindle, embezzle, and blackmail property in order to maintain a livelihood, seeking ease and comfort, repaying gambling debts (Parker 1998), or avoid payment. In Morgans v. Director of Public Prosecutions,[117] the accused used the telephone line to acquire unauthorized access to the computer systems of several different companies, thus obtaining telecommunication services without payment. In the face of deliberate financial hackers, even the most secure systems on the Internet are meeting universal threats.

In fact, financial hacking is not always as sophisticated as imagined by the

[117] [2000] UKHL 9; [2000] 2 All ER 522; [2000] 2 WLR 386; [2000] Crim LR 576 (17th February, 2000). The conviction was overruled due to the matter of obtaining the evidence, which was obtained through the installation of an interception device into the telephone line of the accused.

public, for sometimes hackers may be the software provider. This is a serious threat for the banking system.

(11) Hacking for educational reasons

This kind of hacking is the unauthorized use of the systems for educational purposes. In the early stage when computer hardware, software, and network services were expensive, they could only be obtained by a limited number of big organizations and universities. Many hackers tried to use the system for educational purposes without permission. Nevertheless, with the development of less-bulky, low-cost personal computers, this kind of educational hacking has become history.

(12) Changing academic results

University students hack for better scores or grades in academic records. In August 1977, officials at a large university in the U. S. uncovered a scheme involving payments by students who wanted their grades altered in the school's computer centre. Investigators found that several thousand dollars had been paid to a university employee who made changes on grade cards that were later used to make entries in the university's computer.[118] From then on, dozens of students in the U. S. have been caught hacking into school computers to give themselves better grades. In one case, nineteen students were suspended after being accused of knowingly involved in electronically changing their transcripts. Seven other students were told their grades were altered. Nevertheless, this was apparently done without their knowledge.[119]

---

118 Lehigh University Uncovers Payment to Alter Grade of Student, New York Times, 1 September, 1977, A-18.

119 C. Anderson, Hacking the Grade, Originally Aired, 3 September 2002. Retrieved 15 February 2016, from

(13) Harassment and murder

Internet harassment can occur in nearly every Internet service to direct obscenities toward others, and make insulting statements based on gender, race, religion, nationality, or sexual orientation (Kelly 2002). In offences where information systems are used as means of committing verbal assault, threat, harassment, alarming, spam and fraud, the motivation of the perpetrator is to harass and to kill the victim. The function of the Internet as a means of communications and with a high anonymity of interaction often entraps the victims into unforeseeable dangers. In 2005, China Ministry of Public Security investigated 1,000 assassination cases, in many of which the criminals found the potential victims through the Internet (Yi 2006). In many criminal cases, stalkers and murderers find and entice victims through the communication and interaction of various Internet services.

(14) Launching political movement

For many years, defence forces, governments, and even computer companies have been popular targets for sabotage attacks. According to Daler and co-workers (1982), political groups in France repeatedly damaged computers, asserting that computers were the favoured tools of those who dominate. Italy, the former West Germany, the U. S., the U. K., Japan, and the Scandinavian countries have experienced sabotage as well, with both the old- and new-fashioned attacks on malicious programmes (Daler and co-workers 1982, pp. 24-25).

Political hacking also formed an extreme movement: “hacktivism”. Hacktivists launch politically motivated attacks on public web pages or e-mail

---

http://www.techtv.com/cybercrime/internetfraud/story/0,23008,3396685,00.html

servers (Vatis 2000). In 1999, for example, the homepages for the White House was attacked by political activists protesting against the site's politics.[120]

(15) Launching cyber warfare

People worry that the threat of cyberwarfare will be a future nightmare because hacking communities have the ability to launch destructive attacks on computer systems. In recent years, a cyberwar was nearly taking place. In 1990, a hacker organization "Legion of the Underground" declared war on some countries in retaliation for human-rights violations. Several other hacker groups condemned the aggressive act, and soon after, the Legion of the Underground retracted their declaration of cyber war.[121] Cyberwafare also happened in the initial years of the twenty-first century. Hacker groups became popular in East Asian countries during several cyber wars, mostly between hacker groups of different countries due to their positional differences on some international affairs. At that time, the relevant countries were highly vigilant to potential abuse of computers and networks and invested more heavily on information security control.

(16) Carrying out anti-computer actions

As some people are against mechanicalization, electronization, industrialization, modernization, and globalization, others are against the process of computerization, informationization and networking. According to Parker (1998), some hacker sympathizers describe attacks as justifiable protests or direct action against enemies of the environment or of society in general.

---

120 See U. S. Department of Justice, Congressional Testimony on Cybercrime Strategy, 28 July 2000.

121 For the story, see Palczewski (2001). For the joint statement, see 2600 and co-workers. Joint Statement Condemning LoU Cyberwar, *2600 News*, 7 January 1999. Retrieved 15 February 2016, from http://www.2600.com/news/view/article/361

Unabomber represented another kind of anti-computer "hacking". He carried out 16 bombings, which, altogether, killed three and injured 23 people.[122] His "Unabomber Manifesto" claimed that technological progress brought about undesirable requirements for the people, and that the people could stop this situation so as to recover their happier and simpler life close to nature (See Kaczynski 1996). Some other activists all over the world also destroyed a number of computers to protest against a computer society in which they thought that computers were being used to control people.[123] Indeed, they were not hackers in cyberspace, but traditional style bombers in real society.

(17) Mimicking cyber Robin Hoods

Orthodox hackers hack in order to make programmes or information available to others free. As a hacker, Maelstrom, stated in an interview that he had never any feeling of moral apprehensiveness when he made Internet access accounts available to the public for free through hacking (Jordan and Taylor 1998, pp. 768-769).

Whether some charitable concerns or individuals will also crowd online to hack for money is an unanswered question. A hacker initially wanted to test how the security level of the mobile communications networks. After he found that he could make money through selling the cards with revised passwords, he opened a specific bank account in which to deposit the money, a separate account from his own daily-used bank account. He said that he did not hack for

---

[122] The offences were carried out during 1978 and 1995. As of 2004, Kaczynski was serving a life sentence without the possibility of parole in a maximum-security prison in Florence, Colorado.

[123] The French activist group called CLODO (Comité de Libération ou de Détournement des Ordinateurs), committed the offence between 1979 and 1983.

himself, but for the wellbeing of others. He donated 200 Renminbi Yuan (about 20 euros) to a leukaemia patient (Gao 2006).

Cyber Robin Hoods do not always publicize their intent. But on some web sites, methods for counterfeiting money are published.

(18) Practising unfair competition

In order to enhance competitive capacity, businesses also engage in attacks against competitive rivals. In the 1990s, when the Internet economy boomed, many big online enterprises secretly attacked the web sites or defame the reputation with each other. Attackers benefit from the decline of competitors and from the increase in their own market share. They even practice access to each other's computer systems to obtain business secrets. In the rapid development of the information market, such destructive or espionage activities are fatal to the victimized enterprises.

(19) Practising trap marketing

Some anti-virus compilers plant computer viruses and other destructive programmes into their anti-virus software to force users to purchase the upgraded versions of anti-virus software they compile or sell. By doing so, they hope to increase the market share and sale of their own products (Jiang and Yu 1997, pp. 18-27). Web sites owners also frequently use this trap marketing. Cookies are an example that is widely known and accepted. In malicious marketing cases, some web sites infect users' computers with embedded harmful codes and instruct the users of infected computers to visit their web sites repeatedly and to pay for cleaning the computer. Other forms of entrapment also include kidnapping computers or programmes in order to render the machine repeatedly operating in a way benefiting code writers or spreaders. Web

browser manipulation is one such abduction that controls the homepage, or even the whole browser, and is directed solely to the perpetrators' web sites.

(20) Strengthening self-defence

Hacking has also been used for self-defence. For example, in order to prevent illegal replication of software, a pair of Pakistani bothers bundled "Brain Virus" into their software and attacked Delaware University in October 1987 (Forester and Morrison 1994, p. 93). Their idea was that only those who pirated the software would be victimized, the virus being an automatic retributive tool. The followers of a religious cult in an Asian country also attacked the satellite communications systems as a means of self-defence. The government charged the religion with being an "evil cult" and prohibited its practice. In revenge, members of this forbidden religion used the Internet to hack several times into the satellite broadcasting system, and changed the official TV programmes to video programmes disseminating the "truth" about this religion.

The idea of the above-mentioned "Pakistan virus" is not without descendants. Many trial versions of software (or shareware) include similar idea in expressive form. While some of the trial versions can work in one way or another after the trial period, other trial versions can be completely disabled. For example, a certain kind of operating system provides a 30-day trial period, after which the system cannot be operated without registration, which implies a process of purchasing. Without the operating system, the computer is simply broken down --analogous to an attack launched by a logic bomb, except that it is an "attack" under the cover of failure to register after the trial period.

(21) Hacking for recreation

Both recreation and hacking are exciting. Randall and co-workers (2000) found that excitement was a major reason for hacking. Here, hacking has an equivalent function to entertainment. Although computing is different from gaming, the computer has a close relationship with gaming. Not only are computer and online games prevalent, but the use of the computer and the surfing of the Internet may serve gaming instinct. Many users enjoy online surfing, interaction and self-publishing, but fewer experience success in accessing and controlling others' information. But by overcoming the slight difficulty in cracking users' password or other access-control measure, a unique pleasure is afforded to users who experience this victory.

(22) Employment-related hacking

Although considerable hacker activities are in fact illegal, the successful hacker will usually be admired for his or her skills. At the same time, many hackers have been offered a well-paid job as a computer expert or even security manager. For example, Robert T. Morris, was one such. He created the Morris Worm in 1988, infecting about 6,000 computers and causing losses that ranged from 200 to 53,000 dollars each. At present, on his web site, he writes that: "I'm at the MIT Computer Science and Artificial Intelligence Laboratory…"[124]

Banks (1997) related hacking to employment, which means that if the hacked system owners caught the hacker, they would employ the hacker exactly to protect the systems from other intruders.

A high-profile employer can employ a hacker who has damaged thousands of computers and caused losses of millions of dollars, a natural analogy is that a better chance of employment should be hacked together through millions of

[124] Retrieved 15 February 2016, from http://pdos.csail.mit.edu/~rtm/

computers, and billions of dollars of losses. Alternatively, less skilful hackers might try to damage some hundreds of computers and obtain an ordinary job offer. Criminal hackers are usually better off after their hacking activities have been made public.

By saying this, we are not making complaint about a function of the judicial system that allows the rehabilitation of those who have committed offences in this way. In contrast to the ideal "general deterrence," the question arises as to whether such a practice serves a generally-motivating role.

Employment-related hacking is not limited to getting employment opportunities through hacking. Hackers have sometimes hacked as a form of retribution when an employer has not provided an offer. Skeeve Stevens seriously damaged the AUSNET, an Internet company that refused to employ him. He had compromised 1,225 credit cards and displayed a message on the company's homepage in April 1995, saying, "AUSNET is a disgusting network … and should be shut down and sued by all their users!"[125] In addition, in DPP v. Lennon,[126] after being dismissed, the accused had downloaded a mail-bombing programme from the Internet and used it to automatically send about 5 million e-mails to the former employer's e-mail servers. His purpose was to bring in the company into a "mess" and did not think his action was criminal.

(23) Hacking for the hacker community

For those who regard themselves as hackers, "hacker" is a symbol, a label, a banner, a movement, a front, and a centripetal force, regardless of the fact that each hacker, particularly each of the malicious hackers behaves in a pattern that

---

[125] Phrack Magazine, volume 8, number 53, 8 July 1998, article 14 of 15, 0Xd.

[126] Director of Public Prosecutions v Lennon [2006] EWHC 1201 (Admin) (11 May 2006).

is not necessarily the same. Therefore, the hacker community is in reality a symbolic clan in which members "hack" in variant ways and for different ends.

Regardless of the fact that the members of the hacker community are heterogeneous, cases where hackers have united to take actions against legal or administrative measures targeted at certain "members" of their "hacker community" are not rare. The mere name of "hacker" may serve to raise an emotive force capable of bringing all kinds of hackers together, including traditional hackers, and hackers who are regarded as cybercriminals. In fact, in such a case, their activities are unreasoning: on the one hand, the activists do not belong to a single group; on the other hand, their targets are far from being only the web sites of the law-enforcement agencies. Their good will is to maintain the image of a "hacker community" as a whole, to prove their power against traditional government and law enforcement, and to resist an outside invasion.

Sub-culture was a term first used by A. K. Cohen in *Delinquent Boys: the Culture of the Gang* (1955) to denote a group or groups inside the host culture with different values from it, as evinced through their expression in deviant behaviour (Walsh 1983, p. 214). Zheng (2004) attribute this motive to impact of the internal communications of the cybercriminal sub-cultural group. As to the situation in traditional criminal sub-cultural groups, these communications produce coherence inside the group. However, the network exists as a means of communications and enhances the communicative pattern of cybercrime. Intrusion techniques and skills are the just contact-nodes for their members.

(24) Destroying evidence contained in information systems

Information systems usually contain evidence for various kinds of cases, civil, criminal or administrative. The party for whom the evidence is

unfavourable has a motive to destroy it, before or during the search and seizure by law-enforcement agencies. In R. v. Anitta Debnath,[127] after the police began to investigate her harassment of the victim, the perpetrator paid a group of computer hackers to assist her to hijack the victim's e-mail, in order that the victim could no longer access the account.

(25) Sexually motivated misuse of information systems

Sex crimes cover a broad category of deviance. The most frequently prosecuted forms of sexually motivated misuse of information systems are the recording, depositing, transmitting, and trading of child pornography;[128] sexual harassment through communication by using information systems; and promotion of (illegal) prostitution with the assistance of information systems.

(26) Child abuse

Children are vulnerable group of people in society. Although international consensus has been achieved and treaties have been implemented requiring governments to "take all appropriate…measures to protect the child from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse…,"[129] incidents, in which children are abused frequently happen. The abusers are increasingly using information systems to lure children to engage in sexual activity and spread child pornography. For example, in R. v. Kasam,[130] the accused used his

---

[127] [2005] EWCA Crim 3472, No. 200501008A7.

[128] See for example, United States v. Ziegler (No. 05-30177 D. C. No. CR-03-00008-RFC ORDER AND OPINION, 6 March 2007), in which the perpetrator used the company's computer to view, deposit and exchange child pornography.

[129] UN Convention on the Rights of the Child (adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989, entry into force 2 September 1990), Article 19.

[130] 2004 ONCJ 136 (CanLII), Docket: 10018867.

computer to collect hundreds of images and several video clips of child pornography (paragraph 2.5). In one compact disc were found 3,200 images of child pornography downloaded from the Internet (paragraph 2.4).[131] Besides sexual motives, there may also be present violent abuse of the child. These two aspects are closely connected with each other. In R. v. Sharpe, the court held that "the possession of child pornography and associated harms to children is the use of child pornography by paedophiles to groom children into committing sexual acts" (paragraph 205).

(27) Anti-deviance hacking

In both cases of United States v. Jarrett[132] and United States v. Steiger,[133] hackers reported the cases and provided critical evidence for the law-enforcement agencies. They have never appeared before the court or been prosecuted. In other cases, such hackers were sued. In a civil case, Fischer v. Mt.

---

131 The court listed some of the depicted graphic scenes that are identified as child abuse:
" (a) A 6-month-old baby girl with an adult male penis having ejaculated onto the vaginal area of the child;
(b) A blind-folded 4-year-old girl performing fellatio on an adult male penis;
(c) An adult male performing anal intercourse on a 7-year-old girl;
(d) A 5-year-old girl performing fellatio on an adult male;
(e) An adult hand is fondling a 7 to 8 year-old girl who is handcuffed. Several adult fingers are inserted into her vagina and her rectum is penetrated with a long stick;
(f) An 8-year-old girl is at a pinball machine. During the 6 minute video she is fondled by an adult female who undresses the young girl, fondles her and ultimately the adult female performs cunnilingus on the young girl on the pinball machine;
(g) The same adult female takes the same 8-yar-old girl in the pinball video in another video and the young girl is guided by the adult female to perform fellatio on an adult male. The video is entitled R@ygold_the family;
(h) Another video entitled family 10.jpg depicts a 6-year-old girl who is naked sitting on a toilet performing fellatio on an adult male." See ibid., paragraph 2.6.

132 Fourth Circuit No. 02-4953, 3 June 2003.

133 Eleventh Circuit No. 01-15788, 01-16100 and 01-16269, 14 January 2003.

Olive Lutheran Church,[134] other employees in the Church suspected Fischer, a Lutheran minister, of engaging in sexual misconduct. They hired a computer expert to guess the password of the Hotmail account that the minister was known to use frequently. As a result, they cracked the password, looked through and printed the minister's messages, in some of which were included contents about sexual activity between the minister and other men.[135]

(28) Comprehensive motives

In some other cases, the offenders have multiple motives, interrelated or unrelated with each other. For example, in R. v. Geller,[136] the offender possessed 101 pornographic images, chatted with young girls of 13 or 14 years old in order to establish relationships (paragraph 5), obtained 400 credit cards and other personal information through hacking, accessed the Internet for 28 times without paying (paragraph 6), and engaged in activities that lead information systems to malfunction (paragraph 7).

(29) Unclear motive

While many perpetrators act in a way to achieve something or destroy something, others act without reasonable reasons. In some cases, it is impossible to detect an impressive motive from the facts of the offence: the revelation of the abuse of information systems cannot lead to a clue for a useful identification of the state of mind. In State v. Moning, the accused used the computer terminal to obtain access to the database to run a query on the previous drug conviction of his acquaintance. After he printed a copy of the information, he

---

[134] Western District of Wisconsin No. 01-C-0158-C, 28 March 2002.
[135] ibid.
[136] 2003 CanLII 31190 (ON S.C.), Docket: 493.

handed the victim the printout. At this point, the victim became aware of the perpetrator's behaviour and reported his unauthorized access.[137]

(30) (Not motivated but) influenced by psychological depression

In R. v. Taylor,[138] the accused woman illegally accessed the account of a man through computer systems and issued an unauthorized passbook for the account, with which an unidentified man attempted to withdraw £25,000, succeeded in getting £500 in cash but failed to get £24,500 in cheques. The opinion of the doctors showed that the woman was diagnosed as HIV positive during her committing the offence and was in a state of "clinical depression" which affected her judgment about her behaviour and the likely result of her behaviour.

Curiosity is an irresistible mental power, propelling people to know the unknown and to control the uncontrollable, or to destruct the constructed, and to deorganize the organized, whether in the macro or the micro dimensions. Information systems are a dimension which has developed partly under the dynamics of human curiosity and has been threatened partly by this force.

Apart from the abundant findings identifying motives in this study, I found that for many hackers, instead of hacking for something, they have succeeded in hacking and then found something to obtain or destruct. The initial hacking was merely a random activity that accidentally succeeded in furthering additional actions. Successful hacking, it could be imagined, might lead to any kind of sabotage, destruction or vandalism, the obtaining of confidential or proprietary information, acquiring control over a system, and so on. Therefore, we can

---

137 2002-Ohio-5097.
138 [1998] EWCA Crim 1545 (12th May, 1998).

safely conclude that there are hackers who hack out of specific motives, and that there are also hackers who firstly hack and then find opportunities to reach specific goals. For hackers with specific purposes, the hacking process may be a sophisticated endeavour before they take hold of the compromised system, because they have to conquer the unknown continent of security. For hackers with less clear initial purposes without wanting to obtain something specific or destroy something specific, the hacking process may be more straightforward until the system is exploited, because they only harvest from a conquered land. These different hacking models imply that the goals can emerge before the beginning of the initial hacking or after the success of the initial hacking—in the latter case, the attempted hackers are likely to defend themselves by expressing the benign motive of wanting to face a technological challenge or a security loophole rather than by stating a malicious intent of economic espionage or sabotage. In this latter case, the motivation is that of a challenging adventure into the partially unknown.

4.8 Conclusion

Information systems store rich and colourful resources, attracting digital community constructors, conquerors, conspirators and criminals. With one-sixth of the population connected online, with a prolonged online time, and diversified online activities, it is natural that cybercriminals constitute a greater ratio among the Internet users, and that cybercrimes will constitute a greater proportion of the whole crimes. If the unbalanced demographic distribution of computer and Internet users exists within different age groups, the comparison

of their online behaviour is a valuable indicator in finding the reasons for this. The key concern in this comparison is that of the role of juveniles and young adults. Empirical studies have disclosed that youths may have more chances to use computers and the Internet and are more likely to commit cybercrime and be victimized. The natural and social properties of different age groups have been shaped in different ways. Different have been their educational background, financial status, sense of responsibility, family structure, social interactions and interconnections, self-control, psychological make-up, and interest, knowledge, and skills. These distinctive characteristics determine that they are confronted with different chances and challenges in information systems, and in respect of gaining and losses in the online activities. As a result, young people are more likely to be involved in online adventures, stalking or stalked, exploiting or exploited, hacking or hacked.

The internal reasons why criminals are devoted to cybercrime are connected with the functioning of information systems. This shows that the novelty and mobility of information systems enable people from quite different contexts to find something useful, valuable and profitable. Psychological satisfaction, spiritual enjoyment, financial obtaining, winning fame, opportunity getting, and fortune seeking are all realizable through the use and misuse of information systems. The motivations of committing cybercrimes are diversified. This means that cybercrimes are profitable for whatever purposes the criminals are pursuing.

To sum up, the criminals' motives may be satisfied in part by her or his having committed a crime against the person and in part by his having committed a crime against property. And there may be motives that can be

satisfied outside both these opportunities. Motives of likely offenders are different but barely novel (Grabosky 2000, pp. 2-3).

CHAPTER 5 CRITICAL FACTORS IN COMBATING CYBERCRIME

5.1 Introduction

As it was pointed out in "US Cybersecurity: Progress Stalled" that,

"Cybersecurity incidents are not only increasing in number, they are also becoming progressively destructive and target a broadening array of information and attack vectors. It's clear that adversaries continue to advance their threats, techniques, and targets. They are investing in technologies, sharing intelligence, and training their crews to attack with purpose and competence" (PwC 2015, p.3)

Information systems have multiple vulnerabilities, plays multiple roles in cybercrime, while the cybercriminals are themselves have varied motivations. This chapter will discuss critical factors in the fight against such offences. The core question this chapter seeks to answer is the ease in finding cybercrime. The term "finding" covers a wide range of activities leading to punishment: detection, reporting, investigation, prosecution, proving and conviction.

At present, the fight against cybercrime also necessitates better knowledge about the critical factors. For several decades, many commentators have written about the characteristics of cybercrime, and many aspects have been generalized

in the light of the surveys, observation and thinking (Thompson 1989; Sieber 1998, etc.).

The following chapter is designed to make a synchronic inquiry into the characteristics of cybercrime in comparison with traditional offences.

5.2 Victimization in cybercrime

The perpetrator-victim relationship in cybercrime is developed through information systems in a process of human-machine-human interaction. The perpetrator fulfils the first half of the interaction and the victim is imposed into the second half of the interaction. That is to say, the victimization of victims of cybercrime also relates to information systems. Victims are also users whose information is deposited in or published through information systems, whose daily life or operation depends on the systems, or whose welfare is increased through the systems. Like cybercriminals, they are also distributed over an unlimited area.[139] In addition, in cases such as virus attacks, multiple victims can be involved. Thousands or millions of users are also likely to be victimized in

[139] For example, in United States v. Magnuson (Fourth Circuit No. 964957, D. C. No. CR-96-186-A, 24 June 1997), the accused used his home computer to attack one victim's computer servers in seven states. Apart from unauthorized access to information systems, other crimes committed with the intervention of information systems can also involve globally distributed victims. For example, in Bohning v Government of the United States of America [2005] EWHC 2613, the accused exploited the telecommunications systems to contact young girls and arrange sexual relations with them. The police revealed from his laptop computer thousands of images of child and baby pornography. The e-mail and chat messages proved that he had transmitted pornographic material to young girls over the world and incited them to engage in sexual relations with him (paragraphs 2 and 3).

one case even. Individual users usually have a lower awareness of cybersecurity than corporate users, and invest less money and time in maintaining and protecting the systems and less on updating their anti-virus software. Although individual users are more vulnerable to potential threats, their losses are usually neglected and underreported.

Computer networks are not so new, but the pervasive use of them is a recent development. The current generation of people accepts, and depends more on, information systems than previous generations. There exists a clear-cut information generation within the information society. Because more young people use the Internet than the elderly do, it is natural that these youths are more likely to be victimized in cybercrime. Thus to some extent cybercrimes are offences of youths against youths. We do not find a sharp reduction of computer use with the increase in the age of young users. Therefore, it is to be expected that with the increase in age of the Internet users, more victims will also be found in future among older users.

Simultaneously, it is undeniable that with more and more organizations pursuing online businesses and other activities, the likelihood that these organizations will be victimized will also grow. In fact, the victims of the original offences against information and information systems were mainly organizations. In the future, they will still be vulnerable to inside and outside attacks. One advantage these organizations have for protecting their information and information systems is that they have a greater capacity than the individual users to afford the anti-virus, firewalls, other access-control mechanisms and for updating these mechanisms.

It is a trickier question when the online victims are more likely to be victimized in a "voluntary" or "active" manner. For example, the Nigerian 419 fraud victims may transfer a sum of money voluntarily to the perpetrators; victims of date rape may go to meet the potential criminals voluntarily; or users may voluntarily retrieve web pages that contain malicious codes, and so forth. Victims are also more likely to admit their "willingness" or "activeness" and less inclined to report the case.

Actual victimization in cybercrime can be more complex through the extension of victimization. For example, the senders of e-mail messages have adopted clever tricks in soliciting recipients. Opening the messages and the attachments is the first goal of the senders. Generally, they use ambiguous and false sender and subject columns, but ensure that there are valid contents (except messages spreading viruses) to show their offers and set their traps.

Unsolicited e-mail messages can have a broader influence on criminal phenomena, where the question is not only of victimization, but also one of conspiracy. Not only do e-mail communications become an offensive means by which the recipients are victimized, but these victims then serve as part of a conspiracy, for they are seduced to participate criminal operations (Li 2005a, 2006b, 2007b).

In the Internet environment, the most frequent victimization model begins from an exposing of victims to potential threats, which we can call the exposing-victimization model. With this model, the victim of unsolicited messages merely puts his/her e-mail address on the web pages, bulletin-board systems, uses it in the chat systems, or even simply transmits it through the Internet. The exposure is not necessarily a show-off. Rather, it is just a kind of

presence on the Internet literally or digitally, something inevitable. Nevertheless, the exposing-victimization model at least implies that the senders of unsolicited messages could easily get the e-mail address in the same way as other Internet users do, without further efforts in collecting or harvesting these addresses.

In other cases, the senders of messages have a search process, and follow the searching-victimization model. Due to the large quantity of web pages and other Internet-related contents, the direct artificial collection of multiple e-mail addresses becomes inefficient. The senders (here we also imply address providers) utilize specialized software to harvest e-mail addresses from the Internet. This collecting process becomes automatic and efficient. The perpetrators have created the searching-victimization model in sending messages. Besides harvesting, they also use a dictionary attack and/or an automatic alphabetical permutation and combination to enumerate possible usernames in e-mail accounts. These methods can also be categorized into a searching process. For the senders, an e-mail account with a random word might not represent a specified person; but for the recipient, he/she is readily the victim of this unsolicited message with attachment.

The victimization of recipients of unsolicited messages happens without the appearance of the recipients in their e-mail account. The victimization means that their e-mail accounts are being spammed, whether they open their accounts or not. Under current the legal framework, the receiving of unsolicited messages is sufficient to constitute a victimization of the behaviour to be imposed punishment.

However, the victimization of unsolicited messages does not end at the initial victimization. The above-mentioned models could be called the first-level

effects of unsolicited messages. Subsequently, the second-level effects are based on the initial victimization. There are possibly also two submodels: initial victimization-subsequent victimization model and initial victimization-conspiracy model.

The initial victimization-subsequent victimization model happens when the messages include viruses, fraudulent sales of goods, or falsified financing and banking services. The first-level victimization is being spammed, while the second-level victimization is being attacked or swindled.

Second-level victimization is not always fulfilled so simply. There is usually involved an initial victimization-exposing-searching-subsequent victimization process. In the case of the Nigerian 419 fraud, the recipients of the unsolicited messages were firstly victimized by receiving messages of this kind (being spammed). If they took a positive reaction to the messages, they were further exposing themselves to the senders. Upon receiving the recipients' response, the senders further worked on the vulnerability of the recipients and the possibility of obtaining their property. The process of searching and exposing might be repeated a number of times. If the senders succeeded in obtaining the recipients' property, the last stage of victimization would occur and the swindle would end.

The victimization-conspiracy model is realized when the messages include tax evasion services, sales of pirated software, sales of falsified documents, and so on. The recipients of such offers are firstly victimized by the unsolicited messages; and if they participating the illegal operations, they then become conspirators of the senders.

Because the recipients of the unsolicited messages inducing conspiracy in an illegal operation would expect to benefit from the cooperation with the

senders, the senders are more likely to send attractive messages of the above kind. In fact, in Nigerian fraud, the senders are usually personating politicians who want to transfer property (money, diamonds, and so on) to the bank accounts of the recipients. As a result, the "conspirators" of money laundering are finally to be victimized in the trickery.

The phenomenon of unsolicited e-mail messages has further proved the low controllability or uncontrollability of the information-network environment. Any e-mail address is vulnerable to unsolicited messages that are sent to exposed accounts on the Internet or to a supposed account according to the dictionary. For the senders, both ways could be seen as a process of searching. For recipients, both ways could also be seen as a process of exposing. However, these searching and exposing processes have become more abundant and colourful in the Internet environment than during pre-Internet times.

The mere browsing of the web pages is the easiest method to get an e-mail account, but it is less efficient. The sender can also purchase millions of addresses of different interests of users from the specific vendors. At an inexpensive price, the buyer can conveniently reach a majority of these addresses. Besides, address harvesting becomes automatized and prevalent with the help of powerful software. Anyone with a mild computer and Internet knowledge has the ability to master the uncomplicated skills and subsequently collect thousands or millions of addresses with specific software, which can be downloaded from the Internet free of charge or with a small sum of payment.

The exposure of an e-mail account on the Internet is unavoidable, because the exposure is in so broad a sense that everything in the normal use of the account could be seen as an exposing process, including the sending and

receiving of messages; publishing on web pages, chat rooms, and BBSes; providing account information to register in online services; or exposing nothing more than a coincidence with a phrase from a dictionary vocabulary; or merely a permutation and composition of letters and numbers so that the senders are also fabricated. In fact, exposure of a single e-mail account will not be so risky without the harvesting mechanism, because it is an inefficient way of picking up a single e-mail account from the Internet. However, it cannot be ignored because the e-mail account vendors could collect and transfer it in a dynamic process, and finally form a growing account database to maintain their business. The harvesting software and a dictionary attack undoubtedly deepen the victimization of the e-mail account holders.

In general, the exposed e-mail account might face double risks of being victimized: being picked up in a formal browsing of web pages and use of other Internet services; and being harvested and guessed. Compared with daily-used e-mail accounts without showing up on the web pages or other Internet services except merely sending and receiving messages, the published accounts are more likely to be victimized. Therefore, it seems more likely that it is the process of harvesting rather than that of guessing is the one that the vendors of the database of e-mail accounts and senders of unsolicited messages feed on. As a result, the double risks of exposed e-mail accounts are in fact unbalanced risks: the risk of being victimized by collectors and harvesters is far more serious than the threats of the guessers.

Unsolicited messages provide e-mail users with several different choices, either legitimate or illegitimate, either to conspire or to be further victimized by attached viruses or pre-established fraud traps. The majority of messages

granted recipients two alternatives: to conspire in tax evasion, or to be damaged by viruses.

In the case of conspiracy in tax evasion, the senders always provide valid contact methods to induce the recipients to participate in illegitimate activities. These offers seemingly aim to establish a relationship between service provider and clients. Nevertheless, the true effect is that they form a conspiracy. The recipients have to react actively before they become conspirators in tax evasion schemes. The process might involve repeated exchange of e-mail after the initial unsolicited messages. Under these circumstances, the unsolicited messages might be transformed into literally valuable (but morally wrong and legally prohibited) information. Thus, the recipients might be less averse to such messages. Such messages become the means of communication for the trespassers and criminals, hence posing great threats to social-control attempts to frustrate illegal activities.

In the case of viruses attack, the senders exploited social engineering to induce recipients to open the messages and subsequently the attachments, by blurring the sender and subject columns and falsifying the message contents and name of the attached files. These messages do not require replies from the recipients before they cause damage. They are also dangerous for the recipients in the sense that they are harming the recipients' hardware and software, wasting the labour force, and hindering the business.

5.3 Time in cybercrime

All offences happen in relation to a certain time. Information systems make a more efficient use of time, either in positive social actions or in negative social actions. A single cybercrime can be completed in a very short time, say, seconds or minutes. The simplest example is to modify or destruct data in a hard disk. The more complicated example is the possibility of transferring the U. K.'s total currency reserve in 15 minutes to another country (Kelly 2002). General cybercriminal offences can involve tremendous information transmission in a relevantly short period. For example, in R. v. Kirkwood,[140] the accused downloaded 934 computer games and uploaded 592 over a period of three months through his bulletin board, which had specialized in exchanging copyright games.

However, preparation for some kinds of cybercrime may be time-consuming, usually taking several days, weeks or even months. It depends on the attacks projected, the complexity of the process, and the security technology of the targeted users. The more sophisticated the perpetration is, the more time is needed for preparation and processing. The more sophisticated the security measures are, the more time is needed for overcoming them.

Many offences are committed in a particular natural time or social time. Natural time is the time-span depending on the natural cycle, for example, four seasons and 12 months of a year, seven days of a week, twenty-four hours of a day, day and night, etc. Social time is the time span depending on the social cycle, for example, work time and spare time, holidays, etc. Circumstances are particular time-spans accompanied by natural events, such as wind, snow, rain, etc., or social events, such as war, riot, strike, demonstration, etc.

[140] [2005] EWCA Crim 3534 (21 December 2005).

In the traditional crime of bank robbery, robbers have generally to act when the bank is open, when money is in the safe, when money is being transferred by special vehicles. It is not a prerequisite for cybercrime to depend so much on time. In principle, electronic cash can be "stolen or robbed" at any time, whether it is work time or not.

Many traditional offences are environmentally or weather dependent. In the case of cybercrimes, the environment and weather become less important. For example, in traditional larceny, when a thief walks in rainy weather, the footprint may soon be eliminated by water, but the footprint may be left if it is in the snow; the wind may conceal the sound of a footstep, and it may be more difficult to see the thief in the dark than on a clear moonlight night. In the environment of cyberspace, the factor of weather is nearly irrelevant, that is, cybercrimes are an all-weather business. In whatever kind of weather, cybercriminals can sit at a computer and perpetrate whatever kind of activity without fear that victims or the third parties will discover him in person.

Cybercrime can cross time-zones, so that the "time" in a day, measured by the criterion of law enforcement, is not so relevant in the offence. Traditional offences may be committed in different periods of the day, for example, stealing when it is dark, burglarizing when the house-owner is at work, etc. Online illegal obtaining of information and money may not be time-limited. However, due to strict supervision and the monitoring of online activities, the perpetrators may have to avoid the work time.

Once successful, attacks may continue for a long time, for instance, for several weeks or for several months. In the case of pure illegal access and the obtaining of information from computers, the victim can hardly find the

intrusion in the subsequent months. The intrusion may be repeated before the loopholes are fixed. In addition, influences of some kind of viruses on whole information systems may last for several years. Once created, viruses can never be annihilated and prevented from spreading. Although old viruses may become less harmful due to the use of anti-virus, the less protected computers can still be infected in subsequent years. Another example of continuing cybercrime is the Nigerian 419 fraud, which has been prevalent for several decades and is still a big threat to Internet users.

Malicious programmes, frauds and some other cybercriminal tricks, once they have emerged, may be analogous to natural viruses or bacteria. They exist independently despite people's use of anti-viruses, which are like an immunity injection for human bodies. As viruses or bacteria may infect those for whom the injection has failed to take, the failure of anti-viruses may reveal the vulnerability of the systems. The attack happens wherever there is a security loophole.

5.4 Space in cybercrime

Like traditional crimes, cybercrimes are also more or less related to the factor of space. The possibility of the trans-territoriality of individual cases is high.

The phenomenon of cybercrime is distributed everywhere. In some cases, offences are committed in such a way that the activities take place in a

distributed manner. In R. v. Dooley,[141] the court found that such file sharing networks as KazaA could facilitate Internet users to share various kinds of files through changing computers connected to the Internet into servers that were accessible to other members, who then install the same software in their own computers, regardless of the location of the computers.

The frequencies of these cases are different in various regions and countries. The objective description of the global situation proves that though cybercrime is characterized by its universality, it is undeniable that cybercrime cases are rare in some countries. For example in Finland, according to Miettinen (1996), from 1980 to the time his study was published, the officially-investigated hacking cases were only 10-15 in number. Although hacking cases involving one or two million dollars of losses also existed, the frequency and severity of the cases were less comparable with cases that happened in countries such as the U. S. In West European countries, cybercrime is also less serious than in the East European transition countries.

Definitely, cybercrimes also leave some kind of traces in digital form and can be used as clues for a traceback. However, we find that cybercriminals are less anxious about traces of this kind than about the risks of being exposed in person. The straightforward example is a person who will dare to intrude into a computer in a neighbouring room through the LAN, but not dare to enter the neighbouring room without permission to gaze at the computer screen, not to mention operating that computer without permission. If a remote intrusion is in question, such as an unauthorized access from Europe to a computer in the U. S., the user has hardly any fear of being exposed or caught. Therefore, trans-

141 [2005] EWCA Crim 3093 (1 November 2005).

national cybercriminals are less discouraged from engaging in these activities by the deterrence of law enforcement.

5.5 The technological nature

In the new millennium, the information economy is a popular expression used by entrepreneurs, while cybercrime is a popular expression used about the criminals. Many scholars have recognized the intensified technological involvement in cybercrime (For example Conly 1991; Clark 1996; Stephenson 2000; Mandia and Prosises 2003; Mohay and co-workers 2003; Vacca 2005; Johnson 2006). In all cybercrimes, computers and the Internet are used as tools. Even if what is in question is an attack where computers or networks, or information is targeted, the necessary tools are still computers and the Internet, without which the offence may fall into the traditional offences, and cannot be classified as cybercrimes. However, technological involvement is a necessary but not sufficient condition. Illegally assembling computers with market traded computer parts can hardly be a cybercrime. Yet, illegally manufacturing computer chips can be. Definitely, if traditional forces and technological means are combined in a certain offence, both cybercrime and traditional offence can run together. For example, a bank employee may be abducted and forced to reveal the IDs and passwords. The combined use of these means is not rare in practice.

Certainly, the computer may not be the only tool in a certain cybercrime. For example, wireless networks and mobile networks provide particularly

complicated ways of making a command to launch an attack.

The extent of technological involvement is different in various cybercrimes, from simply cracking a less complex password to controlling thousands of bots all over the world to launch distributed denial of service attacks. The situation is, regardless of whether straightforward or sophisticated techniques or instruments are used in illegal activities, the damage can always be substantial. Although the overall losses of computer misuse are difficult to calculate, the losses of a single victim may be overwhelming, particularly when an individual does not keep separate back-ups. An attack, even by a straightforward technique, can also result in serious consequences in considering the various detailed situations of victims.

In cybercrimes, in addition to the possibility of manoeuvring multiple computers, the available tools, means and functions are also numerous. In fact, much malicious software can be downloaded from the Internet. Many hacking techniques can be learned online. There are opportunities to purchase a malicious programme from the Internet as well.

5.6 The complexity of cybercrime

The Internet allows for the communicating and planning of criminal activities in more different ways than in even the recent past.[142] The Internet

[142] Lenk (1997, pp. 126-135). The evolution of the attack mechanism in 1982 is password guessing, 1984 Self-replicating code, 1985 password cracking, 1986 Exploiting known vulnerabilities, 1988 Disabling audit mechanisms, 1989 Use of back doors in programmes, 1990 Hijacking sessions, 1991 Sweepers, 1992 Packet sniffers, 1993

also accommodates exchange of cybercrime methods free of charge, or provides sales of malicious programmes (Behar 1997, p. 66). Advanced criminal mechanisms enable the attackers to avoid prosecution or complicate investigations in a straightforward manner (Sofaer and co-workers 2000). This further enhances their universality and concealment, making law enforcement more and more impossible.

Furthermore, imagine the time when there were only 20,000 computers connected to the Internet globally, Stoll (1988) described the process to trace the break-ins by a persistent computer intruder attacking Lawrence Berkeley Laboratory (LBL). The traceback took nearly a year of work apart from requiring the cooperation of many organizations including the U. S. FBI and the German Federal Criminal Police Office, during which the intruders continued their activities against 450 computers and successfully gained access to more than thirty (Stoll 1988, pp. 484-497). Even then because of the complexity of the cyber environment, investigation of cybercrime cases was extremely time-consuming. Since then, for example, the case of Sean Galvez shows a worsening of the situation. He obtained unauthorized access to 40 eBay customer accounts and incurred up to 32,000 dollars of fraudulent charges in 2003 could only be indicted in 2006.[143] In comparison with cases affecting thousands or millions of computers, the difficulties in investigating these relatively trivial cases poses the question of how the prosecution of a

---

Stealth diagnostics, 1994 Packet spoofing, 1995 Graphic user interfaces for attack tools, 1996 Automated probes and scans, 1997 Denial of service, 1998 Web attacks, 1999 Macro viruses, and 2000 distributed attacks. See Longstaff (1999, 231-255).

[143] The Office of the Massachusetts Attorney General, Boston Teen Indicted on Charges He Hacked into eBay Accounts and Stole Victims' Identities, 5 January 2006. Retrieved 15 February 2016, from http://www.ago.state.ma.us/sp.cfm?pageid=986&id=1576

major case is possible.

Johnson (2006, p. 6) has discussed a digital forensic evidence on both national and international levels, the challenge posed by offences of online pornography, encrypted illegal materials, cyber terrorism, cybercrimes against children, and the exploitation of computer viruses in extortion schemes. He found that the process of searching digital documents was extraordinarily difficult, due to the capacity of rapid transmission, storage in remote machines, encryption, or the use of other concealment methods. In 2002 BCSC 524,[144] the Supreme Court of British Columbia found that 102 gigabytes of data had been recovered through the forensic imaging of computer hard drives, which meant that the printouts of such a volume of data could fill a 12,500 foot high stack of paper. As a result, the work in reviewing the data was time-consuming, and required co-operation from authorities in the United States, Singapore, and Great Britain (paragraph 12). In R. v. Harlos,[145] the police seized from the offender six hard drives containing storage of 920 gigabytes of data, mostly child pornography: totally 3162 photographic images, and 763 videos of child pornography (paragraph 15).

The Internet being a vulnerable infrastructure, all the individual and institutional Internet users are exposed to similar threats of becoming victims of cybercrime. In practice, all cybercrimes are more or less committed through technological means. Malicious programmes and anti-viruses are "weapons" in information systems. Malicious programmes are usually designed and disseminated without rewards, being uncommercialized and unsystematic. Anti-

---

[144] Full citation: In the Matter of s. 490(3) of the Criminal Code and In the Matter of Edmond Edward Edmond et al. 2002 BCSC 524.
[145] 2005 ABPC 118.

viruses are designed and sold as commodities. Both of them are products of labour, but with a different use: the former being offensive weapons, the latter being defensive weapons.

McAfee (2005, pp. 2-13) has summarized tools and their functions in cybercrime. These tools are used not only to access confidential information, but also to conceal traces, and prevent normal functioning. Most of these tools can be downloaded from the Internet free of charge or at inexpensive prices. It is especially easy to search and obtain such a programme from the Internet as freeware or shareware using a search engine. Many tutorials are furthermore prepared for non-professionals to study them systematically from primary level.

Compared with malicious programmes, the sources of preventive programmes are fewer in number and more expensive on the market. To search such a programme on the Internet turns out to be more difficult than obtaining are free of charge. The usual results are that the links are redirected to a trial version with limited functions or a full version with payment instructions. The incentives for not revealing such programmes are profits, compared with the incentives for causing broader and larger damage and gaining fame by the revelation of malicious programmes. These cases are akin to cases of copyrights and their infringement.

Both factors, discussed in Sections 5.5 and 5.6, can be simplified because of the abundant opportunities for abuse of information systems. In fact, many practical cases have shown that rather than depending on sophisticated technologies and overcoming complicated processes, the perpetrators simply exploit the opportunities at hand. In Yearly v. Crown Prosecution Service,[146] the

[146] [1997] EWHC Admin 308 (21st March, 1997).

accused, a computer engineer, accessed without authorization a security document in the computer he worked on for a store and he then put it on the Internet. Although his computer knowledge was a condition of his employment, nevertheless, in obtaining the confidential file, opportunity was the most significant element rather than his knowledge and skills. With a malicious intent, everyone with the least knowledge of computer systems but are given the same opportunity would be able to do the same. An offence primarily engenders by opportunity, should not be measured by the sophistication of techniques and the complexity of the processes involved.

5.7 The costs of cybercrime

Although much literature dealing with "the costs of crime" has been written by economists, statisticians, jurists, and sociologists, the practical estimate of the costs of one single offence or the whole criminal phenomenon has proved impossible to work out. However, the costs of crime can roughly include direct and indirect costs, physical and psychological costs, and both the costs before the incident and after the incident. There have been efforts to quantify the losses of computer crime, for example Wasik (1991, pp. 34-41), or measuring the size of the problem, for example, Grabosky (2000, pp. 8-9). In respect of the losses caused by cybercrime, it is overall so expensive that no other criminal activity can compare with it. Sometimes, the "losses" of one offence may not necessarily be a pure social cost. Some of the wealth may be transferred from the victim to the offender. Generally, the more the offender

obtains physically, the more the victim loses. In some other cases where the offender does not acquire substantial property, mere "losses" of a victim's money or health satisfy the offender's psychological needs. In both cases, the offender has expected benefits. Again, the more the victim loses or the more seriously the victim is hurt, the more the offender is satisfied psychologically.

Monetary losses caused by crimes, particularly by cybercrimes, are thus difficult to calculate. Direct measurements being unavailable, only some important references can be used to indicate the extent of these losses.

As a first reference, because individuals and businesses have to invest heavily in information security and have to change their behaviour to reduce the probability of being victimized (Gray 1979, p. 13), spending on cybersecurity services and products constitutes, for example, a significant part of the losses brought about by the threats of cybercrime. Without cybercrime, The ICT industries do not require to invest specifically in security protection. In the meanwhile, investment on security protection does not increase productivity. Presently, this expense becomes a necessary part of their ordinary inputs.

The second reference is that losses in individual cases provide a more direct impression. Daler and co-workers (1989, p. 22) reported that the average loss obtaining in a cybercrime case is around 400,000 dollars, as compared with the average take in an old-fashioned bank robbery of 6,000 dollars. The CCIPS web site publishes a list of cybercrime cases prosecuted in the U. S. in recent years. It is obvious that once the cases involve losses, the amount will be large (definitely, there are also cases not involving any monetary loss) (CCIPS 2006). Calculating the 115 cases prosecuted during March 1998 through to May 2006,

the lowest single loss was 5,000 dollars, and the highest was 80 million dollars. The average loss in these cases was 1.27 million dollars (Li 2008a). The losses involved in single cases differ from each other. The media, for example, reported that the infamous Love Bug of 2000, for example, infected at least 45 million computers and caused losses of millions of dollars.[147]

The third reference can be obtained from various cybercrime surveys, each of which provides some information about the situation of the respondents. For example, the annually operated CSI (2005) survey on 700 US computer security practitioners in corporations, government agencies, financial institutions, medical institutions and universities, found that the reported average financial losses resulting from security breaches are 204,000 dollars per respondent. The total losses for 639 survey respondents came to exactly over 130 million dollars (CSI 2005).

Accurately calculating the losses of cybercriminal offences is a task of some sophistication (UNCJIN 1999, Paragraph 27). Cybercrime is a comparatively easy business, but the deterrence, in its turn, is far from easy. Notwithstanding the fact that the whole world is actively combating cybercrime, the number of cybercrimes is still on the rise and their costs are increasing exponentially (CSI 2000). In 2002, the estimation of cybercrime losses averaged about 50 billion dollars annually (Hale 2002, pp. 5-6). In 2005, another estimation of losses reached 400 billion dollars (McAfee 2005, p. 5). The meaning of this number from the year 2005 may be well understood if we compare it with the 9/11 attacks that cost New York City at least 17 billion

[147] BBC News, 4 May 2000. Retrieved 15 February 2016, from http://news.bbc.co.uk/hi/english/uk/newsid_736000/736570.stm

dollars. Further, it may be pointed out that the forecast for the effect of terrorism in general, is a reduction of 0.25 percent of the world economy's growth rate -an impact of around 75 billion dollars (Davidson 2003). If such comparisons are used in measurements, worldwide overall cybercrimes is bleeding the economy of nearly 24 times the sum of the 9/11 attack losses. In addition, companies are investing heavily in a variety of security technologies and insurance (Sofaer and Goodman 2001, p. 5). This is not unrealistic, if we recall that the International Monetary Fund June 2002 Global Financial Stability Report reflects, in a conservative estimate, the total insured losses for 9/11 of around 44 billion dollars (IMF 2002, p. 38). The following table further shows estimated costs of different offenses and percentage of GDP (McAfee 2013, p. 5):

Table 2 Comparison of Costs between Cybercrime and Other Crimes

Putting Malicious Cyber Activity in Context

CRIMINAL ACTION	ESTIMATED COST	PERCENT OF GDP	SOURCE
GLOBAL			
Piracy	$1 billion to $16 billion	0.008% to 0.02%	IMB
Drug Trafficking	$600 billion	5%	UNODC
Global cyber activity	$300 billion to $1 trillion	0.4% to 1.4%	Various
US ONLY			
Car Crashes	$99 billion to $168 billion	0.7% to 1.2%	CDC, AAA
Pilferage	$70 billion to $280 billion	0.5% to 2%	NRF
US- cyber activity	$24 billion to $120 billion	0.2% to 0.8%	Various

Besides the direct cost, Loeb has estimated that breaches of confidence can make companies lose more than 5 percent of their market value on average

(Loeb 2004, p. 69). A survey by Telang and Wattal (2005) analysed the economic impact on 18 software suppliers and found that announcing vulnerability in one of these companies' products caused a 0.6 percent fall in its stock price, or an 860 million dollars fall in the company's value (Telang and Wattal 2005, p. 3).

Immeasurable are the losses of confidential information on state security, governmental reputation and diplomatic relationships. In McKinnon v USA & Anor,[148] the accused obtained control over dozens of computers belonging to and used by the U. S. Government, through which he could gain further control over hundreds of thousands of computers. Among them were 53 Army computers, 26 Navy computers, 16 NASA computers, and 1 Department of Defense computer.[149] Upon gaining access, the accused deleted critical operating systems from some computers, and copied files into his own computer from some other, including passwords, causing a total of 700,000 dollars of loss.[150] Given there was no further loss from his unauthorized access, the U. S. government has been striving to extradite him for prosecution. The visible and invisible losses made the government unwilling to give up the lengthy proceedings in the U. K., even though his conviction can provide no more compensation for the losses.

In recent years, there are efforts to count cybercrime as a percent of GDP (CSIS 2015):

Table 3 Cybercrime as a Percent of GDP

[148] [2007] EWHC 762 (Admin) (03 April 2007)
[149] ibid., paragraph 3.
[150] ibid., paragraphs 4 and 6.

Country	% of GDP	Country	% of GDP
Argentina	N/A	Malaysia	0.18
Australia	0.08	Mexico	0.17
Brazil	0.32	Netherlands	1.50%
Canada	0.17	New Zealand	0.09
China	0.63	Nigeria	0.08
Colombia	0.14	Norway	0.64
EU	0.41	Russia	0.10
France	0.11	Saudi Arabia	0.17
Germany	1.60%	Singapore	0.41
India	0.21	South Africa	0.14
Indonesia	N/A	Turkey	0.07
		United Arab	
Ireland	0.20	Emirates	0.11
Italy	0.04	United Kingdom	0.16
Japan	0.02	United States	0.64
Kenya	0.01	Vietnam	0.13
Korea	N/A	Zambia	0.19

In general, what makes the situation worse is not only that cybercrime is expensive, but also that the costs are rapidly increasing. Only if it reaches saturation point,[151] can the speed of development become stable or commence

151 The original meaning of "saturation point" indicates a situation in which no more people or things can be added because there are already too many. Summers (2003), p. 1457. In research on criminal phenomena, it is also possible to suppose a saturation point where a sharp increase or sharp decrease in the number of crimes no longer occurs. Criminal phenomena can be maintained in a relative stable situation if the forces of crime and deterrence are balanceable in a short term or a long term. Saturation in the short term is always possible. The shorter the term, the more stable the development tendency. Nevertheless, sometimes long-term saturation is also possible, because in the long term, the development tendency line appears flatter than

to decrease. Furthermore, in the "competition" between the criminals and law enforcement, it is obvious that the former are more efficient in obtaining new technologies than the latter (Centre for Strategic and International Studies 1998).

The above analysis concentrates on the general impact of cybercrime on society. A special issue requiring clarification is that of the impact of cybercrime on individual victims, comparing a pensioner and a millionaire both of whom are undergoing 100 euros of losses in a cash card fraud. The direct suffering of the former is definitely far more severe than that of the latter. Criminal justice, equally protecting the poor and the wealthy, may reasonably be considered inefficient in equally treating every euro value of property belonging to every person. In addition, traditional crime can be lethal to natural persons, but has a less severe threat to legal persons in general. However, more and more businesses have considered cybercrime more likely to happen,[152] and more harmful than physical crimes.[153] This is a natural result of increasing importance of information for enterprises and increasing threats of cybercrime to information security.

The following sections will deal with the issue of "the dark figure" of

---

in the short term. What is difficult is to define short term and long term in research on crime. Traditional crime might be placed in a term of a century or millennium, while the development process of new crime should be measured in decades, years, or months. The book does not limit what kind of term is suitable for cybercrime.

[152] IBM. IBM Survey: Consumers Think Cybercrime Now Three Times More Likely than Physical crime: Changing Nature of Crime Leads to Significant Behaviour-Changes, 25 January 2006. Retrieved 15 February 2016, from http://www-03.ibm.com/press/us/en/pressrelease/19154.wss

[153] IBM. U. S. Businesses: Cost of Cybercrime Overtakes Physical crime: IBM Survey Shows Changing Nature of Crime Causes Organizations to Look Inside, 14 March 2006. Retrieved 15 February 2016, from http://www-03.ibm.com/press/us/en/pressrelease/19367.wss

cybercrime. Traditionally, the dark figure has been formed as a consequence of the criminals' self-concealment, family relationship and even from community reasons (Radzinowicz and King 1977, pp. 31-34). With regard to cybercrime, besides conventional concealment methods, information systems constitute another significant mask for perpetrators, a shelter for the criminal, and a tool for hiding traces.

5.8 The anonymity of the perpetrators

Communicating anonymously is a great characteristic of the Internet environment. In using the Internet, anonymity can be kept from the beginning to the end (for an in-depth exploration, see also Li 2014a). First, anonymous access to the Internet poses the most serious threat. In many countries, one of the most important forms of using the Internet is realized through cyber cafés or libraries, where anonymous users can access many of the online services. Definitely, there exist different situations in different countries. Compared with Finland where there are few cyber cafés in towns and cities, the cyber cafés in China have become the "third space" of school-aged juveniles besides home and school. The facilities and services in academic or public libraries are far less convenient for users than those in cyber cafés managed by private firms. An increasing number of hacking cases involving the Internet or Internet users are committed or conspired in cyber cafés.

Secondly, anonymous subscription to the Internet services raises the difficulty of identifying users. The personal information provided for the

registration of an e-mail account, the name and address of e-mail messages, and the authors' information in Usenet, etc., can all be fabricated. Keeping identity anonymous is favourable for the protection of users from victimization, but it also favours the hiding of perpetrators from being traced.

Thirdly, users can keep their identity anonymous in the process of online communications. There are also mechanisms for keeping complete anonymity by which one user can send messages to other users, and then the messages are transmitted to the final target, such as newsgroup, e-mail list, or a single e-mail account. What makes it more complex is that in the mechanisms the intermediary can only be a programme and may be in another jurisdiction (Kingdon 1994). This also reminds us that there exists the possibility of numerous transmitting points, by which messages are transmitted from one terminal to the next terminal, from that to the next in line, and so on, until the message reached the destination.

Tracing this transmitting process is theoretically possible. During the tracing process, the investigation is exactly the contrary to the process of transmission. Each time, the investigator can trace back one point.

It is likely that all points are identifiable. Nevertheless, as long as there is an unexpected element at any point, the tracing chain can be disrupted without reaching the original source. According to National Police Agency of Japan (1998), the possible examples include that the victim has no record of the Internet Protocol (IP) address; ISPs do not keep suitable records; hackers alter the logs; or some points are located in countries that have not criminalized hacking. As Koch (*Inter@ctive Week,* 10 July 2000) has pointed out, theories

about detection remain theories, and they are too new to be tested in practice. Even if all the work of traceback is fulfilled, the actual value of this work may be discounted in a judicial process because of different locations and thus diversified jurisdictions.

Fourthly, the specific service or software can play further roles in hiding users. Cybercriminals usually establish anonymizers, which are systems particularly designed to invalidate technical identification of the source of communications.[154] In fact, this kind of service or software can also be conveniently obtained free of charge or at an inexpensive price from the Internet. Everyone who is online can get access to these tools and services. Such software is likely to be replicated and spread unlimitedly, creating a bigger population of hidden users who potentially threaten the security of information systems.

Although the anonymity of cybercriminals poses a series of questions, it is still the core of the "perfect environment" for the criminals;[155] yet it is at the same time welcomed by Internet users. People are constantly concerned that without online anonymity, it could be impossible to guarantee fundamental rights (COM(2000) 890 final, p. 20; National Police Agency of Japan 1998). It is not strange that the European Union Data Protection Working Party's Recommendation recognized that online anonymity brings about a dilemma for

---

154 See Belgium's answer to the "Questionnaire 5: Have you received any reports from your law-enforcement authorities that have indicated an obstruction of their work due to the non-existence of appropriate legal instruments concerning traffic data retention?" in Council of the European Union, Council doc. 11490/1/02 CRIMORG 67 TELECOM 4 REV 1, Brussels, 20 November 2002.

155 Levinson (2002), p. 455, saying that anonymity is exploited by perpetrators of old crimes such as fraud, pornography, gambling, stalking and identity theft, or new crimes such as unauthorized access, denial of service, and malicious programmes, pp. 455-458.

governments and international organizations:[156] in particular, in maintaining human rights to privacy and freedom of expression, and combating cybercrimes (COM(2000) 890 final, p. 20). Philip (2002) warned that anonymity can provide users with "the courage to do the outrageous and sometimes even resort to illegal activities."

5.9 Hidden victims

Cybercriminals have a greater advantage than most of the traditional criminals in respect of the low probability of arrest and conviction. Many scholars have mentioned this characteristic of cybercrime, as noted in the literature cited in this section. Hatcher and co-workers (1997, pp. 397, 399.) have pointed out that many cybercrimes are not reported. The term "dark figure", used by criminologists to refer to unreported or unrecorded crime,[157] has been applied to denote undiscovered cybercrimes (UNCJIN 1999, Paragraph 30). Many intrusions are not detected for a variety of reasons (COM (2000) 890 final, p. 11). Cybercrimes can well be described as hidden crimes.[158]

At the same time, victims of cybercrime are willing to be hidden victims (Cook 1997, p. 127). The usual "motives for silence" concerning victimization

[156] The Article 29 Data Protection Working Party (2001).

[157] As Radzinowicz and King (1977) pointed out that, "The recorded figures of crime are huge but the reality behind them everywhere looms far larger. The sinister word dunkelziffer (dark figure) was coined at the turn of the century to express this hidden reality." See Radzinowicz and King (1977), p. 42.

[158] Cook (1997) used "hidden crimes" to denote under-reported or under-recorded crimes such as domestic violence, sexual assault, and racial harassment (p. 55-58). He also used "hidden victims" to denote the victims of the "hidden crimes" (p. 127).

may fall into one of the following categories: 1. The idea that the victimization is not worth the mobilization of justice; 2. Involvement; 3. Pressures of fear; 4. The uneasy accessibility of police and court; and 5. The ignorance of events by the police (Radzinowicz and King 1977, pp. 38-40).

In sketching the victim decision-making, Greenberg and Ruback (1985) have established a three-stage model: the victim judges whether the event is a crime, evaluates its seriousness and decides what to do (Greenberg and Ruback 1985, as cited by Feldman 1993, p. 26). Before these stages, one stage that is more important should be added, that is, whether the victim knows the event. If this is the case, the reporting of cybercrime may remain at a lower level, because cybercrime is invisible and difficult to discover; it is more difficult for the victim to judge whether the event is a crime and to estimate the losses; and the victim has less knowledge about whether there is an agency to report the crime. The limited reporting of the cybercrime has been noted more than 20 years ago by Parker and Nycum (1984, p. 313), who studied the invisibility of computer crime. At present, the Internet's virtual environment has made the situation still worse. Fortunate progress in proving material evidences in traditional crimes was made in late 1980s when DNA tests were first introduced (Levinson 2002, p. 537). However, digital evidence in computer crimes is immune from such high-technological testing measures. The invisibility of cybercrimes is based on several factors, either technological or human (UNCJIN 1999, Paragraphs 30, 31). Sometimes, the simple reason is that the victims are not willing to report, or even do not know where to report the case (Salgado 2001). The documented reasons for the reluctance to take legal actions are mainly fear of adverse publicity, public embarrassment or loss of goodwill,

loss of investor or public confidence, resulting economic consequences such as the panic effect that this information would create on their stock prices (See Carter 1995, p. 21; Roush 1995, pp. 32, 34; Gelbstein and Kamal 2002, p. 2; McKenna 2003a), and exposure to future attacks (COM (2000) 890 final, p. 11). The UN suggested that these factors have a significant impact on the detection of cybercrime (UNCJIN 1999, Paragraph 31).

Yet there are other reasons for the victim to keep silence. While many people are active in maintaining their interests and rights, some people view victimization as their own failure in life and career and are not willing to reveal the fact of their failure to any individuals and institutions, so as not to make public their own weakness.

Therefore, it is inevitable that the rate of unknown instances of cybercrimes has increased as a result. The CSI (2005, p. 20) summarized the reasons why the U. S. organizations did not report intrusions to law-enforcement agencies in 2005, including unawareness of law-enforcement interest, a civil remedy seeming the best course, computer would use to their advantage, and negative publicity would hurt the image of their stock. This survey has indicated the percentages of respondents identifying each stated reason as being very important in their decision not to report computer intrusion. At the same time, it is worth noting that the reasons are subject to changes in each annual survey.

5.10 The concealment of cybercrime traces

Mitchell and Banker (1997, pp. 707-711) have concluded that there are four characteristics in which cybercrimes are different from traditional crimes, that is to say, difficulties in detection, limited reporting, jurisdictional complexities, and resource constraint. All these four aspects fall under the broad characteristic of concealment. The concealment of cybercrimes has been brought about by other technological and human factors (Conly 1991; Clark 1996; Stephenson 2000; Mandia and Prosises 2003; Mohay and co-workers 2003; Vacca 2005; Johnson 2006).

Most of traditional offences are highly visible due to apparent depredations, presence of witnesses, and so on. There are also traditional crimes that occur in private places and become less visible (Walsh 1983, p. 236). Unlike traditional threats where criminals are physically present at the crime scene, cybercriminals are usually not present at the crime scene thus making apprehension difficult (Speer 2000, p. 260). In information systems, executing a command to delete files does not mean that the files are permanently deleted. What happens is merely that files are hidden due to a change in file names so that the files can be recovered,[159] except when a secure-eraser programme is in use.[160] Skilful criminals can disable this kind of security mechanism, and conceal

[159] In United States v. Angevine (Tenth Circuit No. 01-6097, D. C. No. 00-CR-106-M, 22 February 2002), "the computer expert used special technology to retrieve the data that had remained latent in the computer's memory," though the accused had attempted to delete the relevant files. In United States v. Upham (First Circuit No. 98-1121, 12 February 1999), the investigator used the "undelete" function of a programme to recover deleted files from the deposit media, as primary evidence in conviction. In Robertson v. Her Majesty's Advocate ([2004] ScotHC 11 (17 February 2004)), the police recovered 347 deleted images from the unallocated space, and 878 images and 45 movies from deleted zip file within the disc.

[160] See for example, International Airport Centres, L. L. C., et al v. Jacob Citrin (Seventh Circuit No. 05-1522, 24 October 2005), p. 2.

the data that might possible be taken as evidence in prosecution.

Technological advances have both a positive impact on businesses and a negative impact on law enforcement (Institute for Security Technology Studies 2002). For example, in the DrinkOrDie case, the online software piracy group concealed its actions by various security measures: exchanging e-mails via private mail server using encryption; using a nickname to identify members, and communicating about group business only in closed, invite-only IRC channels; the FTP sites, where tens of thousands of pirated software, game, movie, and music titles were deposited, were secured by particular authentication mechanisms (U. S. Department of Justice, Press release, 17 May 2002). On the other hand, the available technological solutions have not completely met the requirement of data collection, log analysis, and Internet protocol tracing (American Society for Industrial Security 2004, p. 40). There is also the necessity for law-enforcement agencies to recruit personnel with "electrical engineering and computer-science backgrounds" (Fields 2004, p. B1);

Inevitably, critics point out that cyber police have extra incentives than combating cybercrime, for example, asking for more money, more wiretap, bugs in computers and sell phones, weak encryption and permission to implement security technology, without more arrest following (Koch Inter@ctive Week, 10 July 2000).

Concealment of crimes has important economic effects. Stanley (1995, p. 2) stated that concealment of crime can decrease the incentives not to perpetrate, and increase the costs of law enforcement. Concealment of cybercrime demonstrates the low probability of punishment. In the U. S., only one in 100 cases was detected, one in 8 prosecuted, while only one in 33

prosecuted cybercrimes resulted in a prison sentence. That is to say, the likelihood that a cybercriminal would be put into prison was a one in 26,400 chance (Daler and co-workers 1989, p. 22), as compared with the likelihood of imprisonment in traditional bank robbery a one in three chance (ibid.). Law-enforcement agencies found that a majority of cybercrimes never reached the criminal-justice system. Even in the relatively few cases where a crime was reported, most often the criminal's identity was never discovered.[161] As a consequence, as Radzinowicz and King (1977, p. 67) pointed out, "The calculation of chance is as applicable to the commission of crime as to many other activities." Given other factors constant, if cybercrime is more concealed than other offences, the potential perpetrators are more motivated to take illegal actions on the Internet, and thus more offenders of traditional crime will be prepared to migrate to cyberspace.

5.11 The trans-territoriality of cybercrime coverage

Free flow of information from one country to another is a goal of information systems,[162] but trans-border flow is not free.[163] The trans-border information flux is accompanied by risks of crime of a similar nature. In any

---

161 Phrack magazine, Identifying Net Criminals Difficult, volume 18, number 53, 8 July 1998, article 14, 0X1. Retrieved 15 February 2016, from http://www.phrack.org/phrack/53/P53-14

162 Directive 95/46/EC, Preamble (3); UN A/RES/51/162; Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Article 12.

163 The Convention mentioned above, Article 12 provides the limit on trans-border transfer of data.

country, the court must have jurisdiction over the person or the subject-matter of a lawsuit. This works well with the current set-up of law-enforcement agencies that are territorial and are operating in different villages, towns, districts, cities, counties, states or provinces, or national boundaries. Nevertheless, unauthorized access to information systems can be accomplished from virtually anywhere on the networks, [164] because the communications capability of cyberspace allows criminals to conspire more easily, without geographical proximity to one another or to the target (Lenk 1997, pp. 126-135). The international characteristic of cybercrime is evident (National Police Agency 1998). Cloud computing poses even more challenges on law enforcement, because it is often not obvious for criminal justice authorities in which jurisdiction the data is stored or which legal regime applies to data (Cybercrime Convention Committee (T-CY) 2015). In fact, some of the cases prosecuted have been of this nature, for instance, R. v. Kozun,[165] where the forensic analysis of the computer of the accused disclosed that 165 separate users from 15 countries had traded through his computer. The computer was converted into an automated trading centre through a programme, by which 141 users had traded in the previous 13 days.

The sphere of legal jurisdiction makes the cybercrime enforcement more complicated (Lee and co-workers 1999, p. 873). Smith, Grabosky, and Urbas (2004) concluded that the trans-national dimension of cybercrime posed four

[164] See cases such as United States v. Tenebaum (Israel), 18 March, 1998, involving an Israeli hacking United States military computers; United States v. Gorshkov (W.D. Wash) 4 October 2002, Russian hacker; United States v. McKinnon I (E.D. Va.) and II (D. N.J.) 12 November 2002, British National Hacked into the U. S. Military Networks; United States v. Zezev (S.D. N.Y.) 1 July 2003, Hackers from Kazakhstan; United States v. Ivanov (D. Conn.) 25 July 2003, Russian hacker.
[165] 2007 MBPC 7.

formidable challenges for prosecutors, who have to determine whether the conduct in question is criminal in their own jurisdiction, collect sufficient evidence to mobilize the law, identify the perpetrator, and determine his or her location, and decide whether to leave the matter to the local authorities or to extradite the offender (Smith, Grabosky and Urbas 2004, pp. 48-49).

Sinrod and Reilly (2000, p. 2) have pointed out that although some international organizations are examining cooperative mechanisms in the field of fighting against cybercrime, many of their members are slow in recognizing the urgency of the situation.

The elimination of borders favours inter-jurisdictional mobility of crime. Due to the actual difficulty in establishing jurisdiction, even if a certain offence is detected, it is still uncertain whether the way can easily lead to punishment.[166] Reasonably, suggestions have been made to incorporate cyberspace into various jurisdictional frameworks. Nonetheless, this needs a great deal of time, agreement, and co-operation between countries, which are still struggling to take common actions.

Finally, it is worth noting that trans-national cases only constitute a minor part of cybercrime (Li 2008a). No certain conclusion can be drawn because it is

166 In R. v. Burns ([2003] NICC 13(2) (12 September 2003)), where the accused cloned mobile phones, or exploited faults or loopholes in the internal phone systems of companies or organizations to make cheap or free calls at the expense of those companies or organizations, the court found that:

"As the investigation progressed it became more wide-ranging and involved another suspect and its ramifications were such that it eventually spread to other parts of the United Kingdom, to Tokyo, to South America, as well as to New Jersey and Atlanta in the United States of America. Several large organizations in the United Kingdom, other police forces and international telephone companies were involved. When it became apparent to the police that they did not have either the specialist equipment or the necessary expertise to access much of the information, specialist firms had to be engaged. All of this took a great deal of time."

possible that trans-national offences are not as prevalent as scholars have assumed. On the other hand, it is difficult to reveal these offences for reasons that scholars have laid bare. Or, it may be, that it is simply law enforcement does not put sufficient emphasis on these offences. Before credible data are available to give an answer to this question, we have certain reasons to claim that trans-national offences have sometimes of a dual nature: they do not appear as prevalent as domestic offences, but they are more difficult to detect and convict. In addition, because the investigation of trans-national offences is more expensive and time-consuming, law enforcement will not give more priorities to these offences than to cases that have happened "close to home".

5.12 The rampancy of cybercriminal phenomena

On the computer age, Bequai (1978, p. 4) said, the computer was a gigantic calculator enabling people to gain large quantity of data by pressing a button. When the computers are connected as a colossal network, "buttons" are used not only to acquire and transmit data, but also to replace some of the traditional interpersonal communications and social interactions. Collin (1999) explained the sense of the virtual world, being "symbolic - true, false, binary, metaphoric representations of information - that place in which computer programmes function and data moves." Cyberspace has developed into a stockroom of the wealth and power of the information age (The London School of Economics and Political Science 2001). The pervasive application of ICT can be regarded as a magnitude change of the contemporary society. It

poses new challenges to the traditional conception and system from many aspects, and it changes the routine activities of a large population of the members of society. This change, among other effects, will benefit the disorganization of the traditional social structure and thus increase the presence of motivated perpetrators and the exposure of their victims. As a phenomenon long existing in society, crime has transformed its forms and grown steadily in different historical periods. Criminal phenomena have always gone beyond the law. New forms of crime will inevitably emerge from a continually developing society, while the law is not ready to guard against them. The requirement for punishing crime requires a revision of criminal legislation and a renovation of criminal justice. The persistent extension of the ranges of crime can but result in the constant extension of the regulating domain of criminal law.

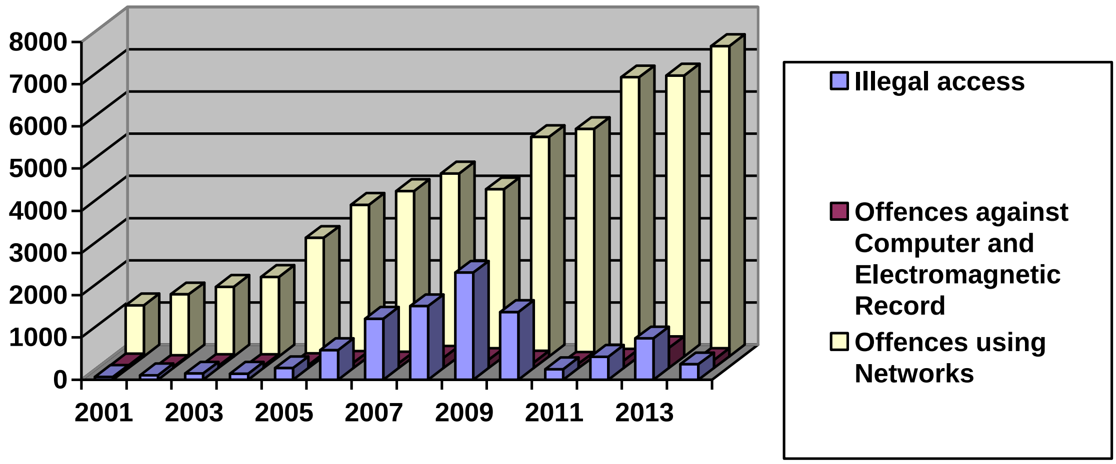
People longed for the industrial society in which their economic situation would be improved, the education level enhanced, consciousness civilized and traditional crime decreased. However, not only has traditional crime not decreased, but also white-collar crime came into being. Where white-collar crime was the offspring of an industrialized civilization, cybercrime concomitantly grew in hand with an informationized civilization. The unprecedented combination of crime and computer creates a stage of anti-productivity, undermining the magnificent prospects for high technology. Criminals abuse the conditions of the emerging market and technologies.

The rise and prevalence of the Internet has become the prominent intervention factor in the development of cybercrime in the recent decade. On the Internet, exist universal contradiction and contention, use and abuse, defence and offence, ethic and deviance, fact and falsification, order and

disorder. The powerful software and hardware that enable people to work more effectively is difficult to operate securely (Allen 2001, p. 2). Speedy technological evolution makes the vendors concentrate more of their time on the market, and less time on security features (Pethia 2001). Although computers and networks are at present protected by various means, the emerging vulnerabilities are inevitably increasing.

All these considerations concerning criminal phenomena in the background of high-technology development does not imply that it is the technology that brings about more crimes. Nevertheless, we cannot deny the factor that the adoption of the new technology may make the crimes more profitable, and less risky (Daler and co-workers 1989, p. 21). Even worse, the criminal will tend to repeat his or her criminal acts-- especially when there is little chance of being caught or convicted. Consequently, cybercrime would pave the safest way to illegal profit, considering the ease with which it can be committed and the negligible chances of imprisonment (Daler and co-workers 1989, p. 21).

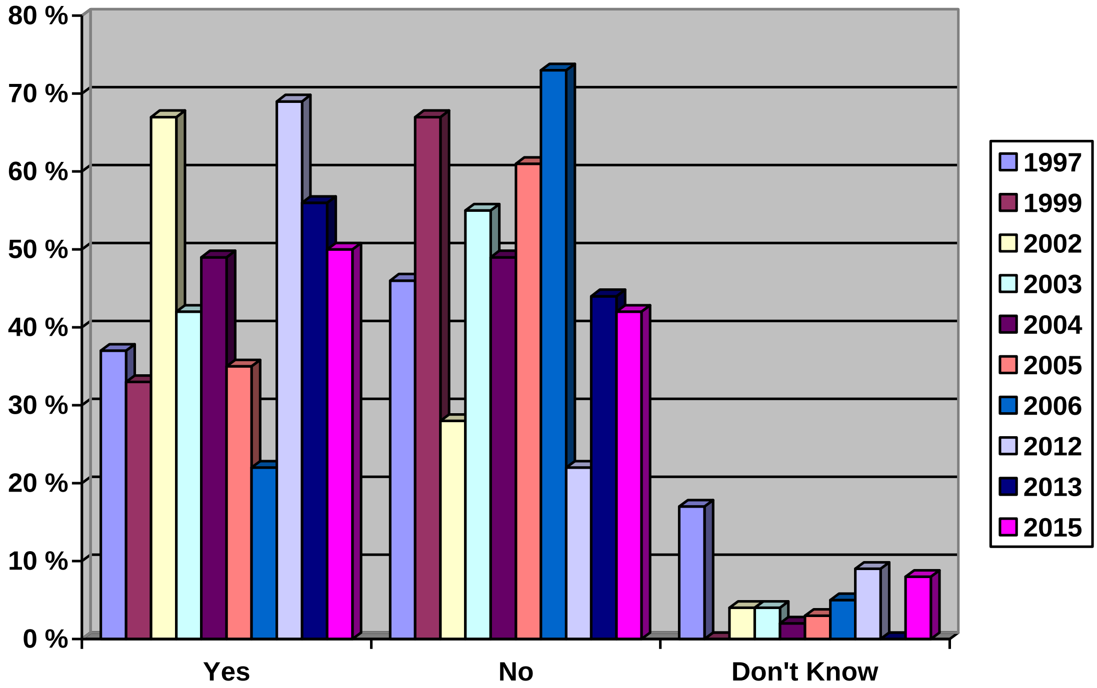
Comprehensive statistics on cybercrime incidents and their impact are not obtainable. However, we can roughly confirm the developing tendency with some available information. For example, arrests for cybercrimes are statistically growing, just to take Japan as an example. There, the total number of arrests of cybercriminals increased from 913 in 2000 to 2,081 in 2004, while it reached 1,612 in the first half of 2005 (National Police Agency 2005).



Illustrated according to the statistics of the Japan National Police Agency, Concerning the Situation of Arrests and Consultancy of Cybercrime, available at http://www.npa.go.jp/cyber/statics/index.html

Figure 2 Arrests for Cybercrime in Japan during 2001-2014

The findings of the cyber security and cybercrime survey are another way of viewing the situation. Australia and the U. S. have carried out annual survey for years. In Australia, the ferment years when the organizations surveyed experienced incidents or attacks against their information systems were 2001, 2002, and 2003 (the answers in Figure 3 were given one year later).



The above figure is based on the statistics from the Australian Computer Crime and Security Survey, collected in 1997, 1999, 2002-2006, 2012, 2013 and 2015. The figure presents the answer to the question "Did your organization experience computer security incidents or attacks against its computer systems in the last 12 months?" This figure refers to the following reports, even though in each report the results of several years' survey are usually included:

1. Australian Computer Emergency Response Team. 2002. 2002 Australian Computer Crime and Security Survey, p.5.
2. Australian Computer Emergency Response Team. 2003. 2003 Australian Computer Crime and Security Survey, p.11.
3. Australian Computer Emergency Response Team. 2004. 2004 Australian

Computer Crime and Security Survey, p.12.

4. Australian Computer Emergency Response Team. 2005. 2005 Australian Computer Crime and Security Survey, p.13.
5. Australian Computer Emergency Response Team. 2006. 2006 Australian Computer Crime and Security Survey, p.17.
6. Australian Computer Emergency Response Team. 2012. 2012 Australian Computer Crime and Security Survey, p.17.
7. Australian Computer Emergency Response Team. 2013. 2013 Australian Computer Crime and Security Survey, p.23.
8. Australian Computer Emergency Response Team. 2015. 2015 Australian Computer Crime and Security Survey, p.16.

Figure 3 Security Incident Trends in Australia

In the U. S., the zenith years of cybercrime were 1997 to 2002 (see Figure 4, the answers were indicators of the situation of the year previous). Both Australia and the U.S. show a fall in positive answers, but the victimization rates are still high. In Australia, it is around 20 percent. In the U. S., it is around 50 percent. In criminological language, they show a victimization rate of 20,000 and 50,000 per 100,000 populations.

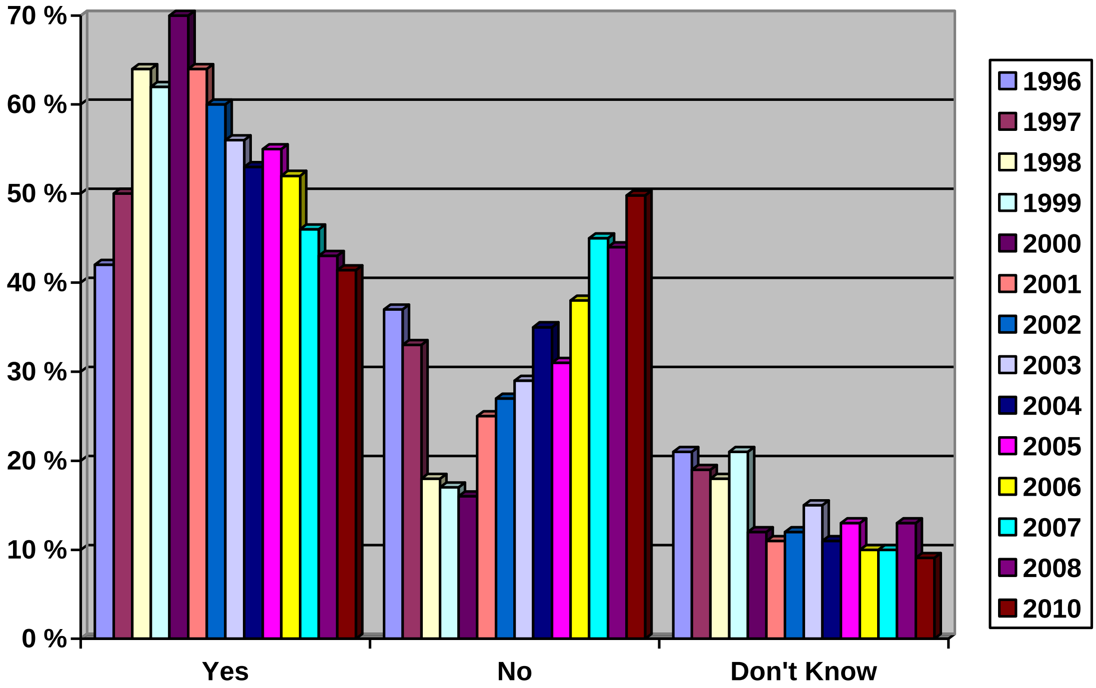


Figure 4 Unauthorized Use of Computer Systems in the USA

The above figure is based on the statistics in the reports on CSI/FBI Computer Crime and Security Survey done annually. The figure illustrates the trends concerning the "unauthorized use of computer systems within the last 12 months" in the USA over the past selected 14 years.

The figure refers to the following reports, even though in each report the results of several years' survey are usually included:

1. CSI. 2000. CSI/FBI 2000 Computer Crime and Security Survey, p. 8.
2. CSI. 2001. CSI/FBI 2001 Computer Crime and Security Survey, p. 4.
3. CSI. 2002. CSI/FBI 2002 Computer Crime and Security Survey, p. 6.
4. CSI. 2003. CSI/FBI 2003 Computer Crime and Security Survey, p. 6.

5. CSI. 2004. CSI/FBI 2004 Computer Crime and Security Survey, p. 8.
6. CSI. 2005. CSI/FBI 2005 Computer Crime and Security Survey, p. 11.
7. CSI. 2006. CSI/FBI 2006 Computer Crime and Security Survey, p. 10.
8. CSI. 2008. CSI/FBI 2008 Computer Crime and Security Survey, p. 13.
9. CSI. 2011. CSI/FBI 2011 Computer Crime and Security Survey, p. 11.

In recent years, cybercrime shows new trends (RSA 2015):

1. The cybercrime-as-a-service marketplace continues to mature.
2. Mobile provides a larger attack surface.
3. Cybercriminals seek more bang for the buck and increase large-scale retail and financial attack.
4. Threats continue to grow more targeted and more advanced.

If we consider that many devices and facilities of the today's society are network-connected today, these trends can be more detailed and concrete in reality. For example, according to Chris Mitchell (2012), a modern car contains networks of communicating devices, which control most aspects of a car's operation, including its brakes, gears, throttle, and engine management. Functionality often also includes external connectivity, e.g. including mobile telephony. This gives rise to a large and varied attack surface, including the following elements. In the US, the mandatory Onboard Diagnostics Unit (OBD-II) port provides direct access to the vehicle's internal network. User-upgradeable systems (e.g. audio players) are routinely connected to internal networks. Wireless devices (e.g. Bluetooth)

are also connected to internal networks. Finally, and most seriously, remote telematics systems (for safety, diagnostics, and anti-theft) provide continuous connectivity via mobile phone networks. A team performed experiments using two cars purchased specifically for purpose. They observed that the car's internal CAN bus has little security – any compromised component can impersonate any other component. There are many other security issues. They demonstrated remote attacks on a car via a broad range of attack vectors, including: mechanic's tools, CD players, Bluetooth and mobile telephony. To perform a mobile phone based remote attack, they reverse-engineered the telematics protocol and used buffer overflow vulnerability in the car gateway to take over the car telematics unit. This attacks works completely 'blind', i.e. without listening to responses from vehicle. Building on this attack they demonstrated the ability to compromise internal vehicle systems, and thereby systematically control the car's engine, brakes, lights, instruments, radio, and locks. The attack could be exploited for theft and surveillance (Mitchell 2012). This remind us that, most of today's vehicles, such as motor vehicles (motorcycles, cars, trucks, buses), railed vehicles (trains, trams), watercraft (ships, boats), aircraft and spacecraft, are more or less assisted by network services and are all vulnerable to various potential cyber attacks. Therefore, there is the possibility that cost of cybercrime can still grow significantly in near future.

5.13 Rent-seeking from the exaggeration of insecurity

The social reaction to and impression on cybercrime are broadly diversified. The general public who are not unfortunate enough to experience or witness real life offences usually rely on the reports of the mass media. While the mass media have their own interests other than maintaining a peaceful and secure daily life, the texts, graphics, audio and video files they compose and create can distort criminal incidents. Some characteristic ways of reporting computer crime have been misleading, even though they play roles in reinforcing the public consciousness of security (Molnar 1987, p. 714). In observing the social reaction to crime, Felson (2002) coined the term "dramatic fallacy" as one of his "ten fallacies about crime":[167] media have interests in seeking strange and violent incidents to keep their ratings high, in which process a highly inaccurate general picture of crime is painted (p. 1).

The tendency to dramaticize and mystify offences that the general public do not often hear about and see stems from the benefits gained by the mass media from their show-off through selective reports. They choose to broadcast what they consider capable of attracting an audience, while at the same time they keep a silence about events in which they have less interest. The most important principle of the media is to be authentic. However, their authenticity is built on selective reports. First identified by Gordon Tullock (1967), rent-seeking finds its way into cyberspace. Anderson (2001) has contributed to the study of exaggeration of cyber insecurity by pointing out in his paper that many interest groups would unavoidably engage in manoeuvring the truth of

[167] These ten fallacies about crime comprise a dramatic fallacy, a cops-and-courts fallacy, a not-me fallacy, an innocent-young fallacy, an ingenuity fallacy, an organized-crime fallacy, a juvenile-gang fallacy, a welfare-state fallacy, an agenda fallacy and a whatever-you-think fallacy. See Felson (2002), pp. 1-18.

the cyber insecurity to benefit from the scared market.

The players may include the mass media, the security engineering community, security professionals, police officers and even professors (Anderson 2001). Schneier (2004, pp.87-89) has criticized the fact that software vendors may have an incentive to exaggerate insecurity. In fact, Hoo (2005, pp. 67-69) has suggested that straightforward, cheap measures are much more worthwhile than large projects that many security vendors prefer to sell. There is definitely a problem that many organizational users leave their computers on and online the whole night after work, many without complex access control. Broadband networks provide a convenience for individual and organization users to keep online 24 hours a day, and seven days a week.[168] Sometimes those who are their contacts can even find their online status in the chat or e-mail systems. The 24-hour-online model is practically more risky than a dial-up service in terms of longer online time.

Doing this research, I have found that many manufacturers of computer hardware and software also have a tendency to provide a darker picture to users when presenting the problem of cybersecurity. This becomes easier to understand when we recall that these manufacturers are striving to survive the growing threats of consumers' awareness against the market of their products. In order not to subject them to product liability, they have to adopt a preparatory stance of impressing the users and judicial organs that the reason for cyber attacks lies not in the defects of their products but in the malicious

[168] Traditional networks are through dial-up connections. Now, two methods of broadband service are digital subscriber line (DSL) and cable modem service. Fiber optics, etc. are gaining ground. See Earthlink Inc. vs. FCC, District of Columbia Circuit No. 05-1087, 15 August 2006.

motives of the perpetrators.

While many people are motivated to exaggerate the truth, Harvey (Financial Times, 3 December 2003) has claimed that cyber terrorism remains an insignificant issue in real life. Evidence can be seen from the detailed documents such as “A Chronology of International Terrorism for 2004”, in which none of the incidents that caused deaths and injuries have employed or targeted computers and networks (National Counterterrorism Centre 2005). In fact, if we consider the urban-crime problem in the U. S., as Miethe (1995, p. 15) did, more than one-fourth of the households were victimized by crime in 1992, while one-half of the population would be victimized by a violent crime in their lifetime. The natural reaction is that cybercrime remains a less than prevalent fear. Although what Wasik (1991, p. 150) suggested that in the future information systems can be used in cases such as murder and injury, the traditional “direct-contact predatory crime predominates” in present society (Felson 2002, p. 23). Apparently, however, the people who are currently engaged in various security services may more easily grasp the more powerful mass media coverage than the traditional offences. The Internet as a part of the mass media airing news about a new computer virus is far more spectacular than what traditional newspapers, radios or TV programme can do about a theft, fraud or murder. By all accounts, most of the current popular knowledge about cybercrime comes from the mass media, regardless of the degree of reliability of such sources.

5.14 Conclusions

According to the basic conclusions of the last sections, we have identified a number of factors that complicate the reporting, detection, investigation, prosecution, conviction, and sentencing of cybercrime. People call for making the punishment fit the cybercrime (Vamosi 2003). However, practicable methods of enhancing law enforcement have not been at hand.

The development of cybercrime necessitates a timely update of the law, as some countries have done. However, it seems that the laws implemented are inadequate for effectively addressing the problem (Vamosi 2003). An example of this aspect can be found in the definition of fraud in U. K. The traditional fraud definition required that a person but not a computer be deceived (Daler and co-workers 1989, p. 125). Thus, the application of fraud provisions has depended on whether a *person* has also been deceived. These authors have mentioned that only in other countries, not the U.K. have the provisions on fraud been interpreted more broadly.

According to the McConnell International (2000, pp. 3-6), only 31 percent of the countries surveyed had substantially or fully updated their laws, 15 percent partially updated, while more than half of the countries had no updated laws. According to the principle of legality, the absence of a law punishing cybercrime sets the deterrent probability at zero, while the actual punishment is also zero. This being the situation, the expected utility of the offender equals the utility when he or she is undetected. By recognizing this benefit, the potential perpetrators will have a greater incentive to commit cybercrime than other offences.

As the conclusions of McConnell International (2000, p. 8) have

demonstrated, light punishments create limited deterrence. The possible reason why creating a virus carries lighter penalties than marijuana offences (McCullagh 2004) may be due to the elasticity of these two kinds of crime from the economists' point of view. Unlike the marijuana offences that are inelastic, cybercrime is more elastic. Tougher punishment for drug crime will be less effective than for cybercrime. However, considering the marginal deterrence when the effect of punishment is too weak to stop cybercrime, this definitely does not deter, either. Lack of a certain degree of severity in punishment will not prevent potential criminals from committing the crimes they are planning, because even if they are probably caught, their expected benefit will still be higher than the expected cost. It is the marginal deterrence of the punishment but not the elasticity of the crime that is working.

However, at the same time, methods adopted in some countries cannot be completely explained by the above theory. Take the example of the application of long-term imprisonment for offences with a low detection probability. The expenses of the long-term imprisonment are quite huge. Thus, it may be said that under these circumstances, governmental investment is insufficient when the emphasis is put on punishment, and detection is ignored. This relates to the value orientation of the government.

Some other countries completely violate the principle of rational choice. They seem to find it difficult to afford adequate funding for detection, conviction, and enforcing punishment, while on the other hand they have established a cyber police, employing huge police forces. The tasks of these cyber police include detection and evidence collection, as well as cybercrime prevention with techniques and human resources, forming a "cyber information

dam". The expense is also huge. As Dnes (2000, p. 75) pointed out, it is of very poor value to increase the probability of conviction through employing more police officers.

In these countries, the concerns about the privacy of individuals have to give way to national security and the maintenance of social order. This means that in the information age, the public organs receive ever greater powers of surveillance and interception. Since the 1990s, the terrorists have frequently launched attacks; and individualism is gradually being submerged by the voice of national interests and international co-operation. The role of punishment in the deterrence of crime is undoubtedly unearthed. Whether in poor or wealthy countries, severe punishment is being used universally for cybercrime. This can be explained as decreasing the expected benefits of cybercrime while increasing the expected costs, forcing the offenders to give up committing the offences and to select instead legal activities. This implies that the means the modern countries take to decrease crime are direct prevention, plus increasing detection probability and increasing punishment severity.

Nevertheless, the following factors deserve further consideration. First, it remains a doubtful question as to whether the information dam can effectively control the information flood. The filtering and blocking of information is expensive and ineffective. As a substitute for severe punishment, it is either a necessary waste of democracy (compared with over-criminalization), or a necessary limit to democracy (compared with information freedom). In order for cybersecurity to be maintained, the private sectors and the public authorities should cooperate to strengthen the legal frameworks for cybersecurity (McConnell International 2000, pp. 8-9).

Secondly, a surer answer can be provided to the question of whether severe punishment is cheap. There have been hundreds of studies done concerning the cost of the death penalty, proving that the death sentence is expensive as well as being easy to execute the innocent. These have become common-sense reasons for repealing the death penalty. The cost of imprisonment is also high. Because the cost of severe punishment is costed differently in different countries, the legislature and law enforcement have a different tendency in implementing various degrees of severity in implementing punishments, which can bring about further jurisdictional problems.

Finally, what should be researched is whether severe punishment is effective. Given that the probability of detection remains extraordinarily low, and that there is no appropriate approach to increase it, a severe punishment again runs up against a limitation. A severe punishment to some extent requires the support of the probability of detection. If not, it loses the basis on which it exists and delivers little deterrence at all.

Cybercrime differs from traditional crimes in its universality, anonymity, concealment, and complexities. While quantitative evaluation of cybercrime has proved difficult, the fight against cybercrime has become a big burden for companies. Because of difficulties in detection, investigation, and conviction, the dark figure of cybercrime remains high. The harsher penalties should be applied to pursue effective deterrence, but in themselves they do not serve protection.

In effect, we are still repeating Radzinowicz and King's dilemma (1977): the perpetrator may escape detection, the detected perpetrator may escape arrest, the arrested perpetrator may not be brought to book due to lack of evidence,

the perpetrator brought to book may be released because his innocent context or trivial offence, the prosecuted perpetrator may escape conviction, and the convicted perpetrator may only be imposed a light penalty (p. 41).

The themes explored in this chapter show that there is no easy way of bringing cybercriminals before the judicial process. Nevertheless, as the next chapter will show, the increase of cybercrime is constant, and the reinforcement of deterrence is a constant need, yet for these two forces to reach equilibrium is still an on-going process.

CHAPTER 6 DEVELOPMENT OF CYBERCRIME AND DETERRENCE

6.1 Basic observations on the development of criminal phenomena

After revealing multi-dimensional obstacles in dealing with cybercrime, this chapter will present a retrospect of the history of cybercrime and relevant legislative and judicial practices.

"History is full of nightmares, some natural, some manmade." (Clarke 1997, p. 223) Nightmare or not, the computer raises problems. The computer was an invention that people could not imagine until it was clear what it happened to be. Before the digital computer had been invented, Thomas Watson, the former chairperson of IBM predicted in 1943 "I think there is a world market for maybe five computers." Although different answers to questions "what exactly is a computer?" and "how many generations of computers have been developed?" are still running parallel,[169] it is widely

[169] According to National Conference of Commissioners on Uniform State Laws, Uniform Computer Transactions Act (UCTA, Amended 2000, 2001), the computer is defined as "an electronic device that accepts information in digital or similar form and manipulates it for a result based on a sequence of instructions." Section 102 (9). However, under different definitions, the computer might be a different device. The general sense of a computer today is a device related to the electronic processing of

accepted that the first electronic digital computer was invented in the 1940s, in the final years of World War II (Hamilton 1973, p. 82). The more notable example is the Electronic Numerical Integrator and Computer (ENIAC), invented in the U. S. in 1946 and since then, according to Tarkhov (1999), computer technology has experienced four generations.[170]

Along with the continuous development of information technology, computer crime may, in principle, have been taking place since the very invention of the computer, but at that time, it neither became a significant problem nor caused great concern. Meanwhile, the development of computer crime should have kept pace with computer technology. The computer developed from a calculator to a word processor to a multimedia device. Besides the research on the history of ICT (Cortada 2002), the history of the computer (Allan 2001; Kuck, 1978, pp. 52-72); the history of the Internet (Okin 2004) or of online information services (Bourne and Hahn 2004), and history of computer ethics (Bynum 2001), scholars have also explored the history of cybercrime (Overill 1998), and particularly, the history of the hacker (Thomas 2002; Peterson 2003; Raymond 2001, covering 1945 to 1990s), or the viruses (Dvorak and Pirillo 2004). Some scholars have researched into the history of

---

digital data.

[170] Tarkhov, S. Generations of the Computers: From Lamp Monsters to Integrated Chips, September 1999. Retrieved 15 February 2016, from http://www.bashedu.ru/konkurs/tarhov/english/generat.htm. The timelines are: 1st Generation in 1950s, 2nd Generation from 1959 to 1963, 3rd Generation from 1963 to 1975, and 4th Generation from 1975 to today. There are also other arguments. For example, Grauer (2001, pp. 7475-7476) argues that the first generation of computers before the 1960s was characterized by electronic tube and later transistors; the second in 1970s, miniaturized integrated circuits; the third in the 1980s and early 1990s, a very large-scale integration of circuits; the fourth since the 1990s, dominated by a very fast growth of Internet users.

the legislation on cybercrime. Ulrich Sieber (1996), for example, concluded that countries have adopted various forms of legislation, and undergone several waves from the 1970s, addressing different problems respectively. They provide a valuable foundation for analysis in this book. The different focuses in these researches do not deliberately furnish any organic links between the development of cybercrime and the development of deterrence. Yet these links are denoted as the primary concern of this chapter.

The chapter attempts to carry out a diachronic inquiry into the history of cybercrime and legislation. Cybercriminal phenomena and the deterrence of punishment through law enforcement and social prevention are undergoing a process of development. The history of cybercrime can roughly be divided into four stages: a stage of germination, a stage of rapid development, a stage of broad expansion, and a stage of routinization. Furthermore, the criminal-law reform relating to cybercrime has never been completely synchronous with cybercrime due to a hysteresis in both the law enforcement and legislation compared with the relevant criminal phenomena.

6.2 Computer hackers' discovery of a lawless new frontier

Upon the hypothesis that computer crime emerged soon after the invention of the first computers, the first stage of computer crime began from the late 1940s and lasted through the late 1960s, when the general public paid more attention to usability, utility, efficiency, and development of the computer, and considered that the computer system was "occasionally unreliable," but

"usually secure" (Dunlop and Kling 1991, p. 524). Unlike today's universal use of computers, there was hardly a computer "market" in this early stage. The manufacture or installation of a computer is an expensive and time-consuming work. However, during this stage, computer crime emerged in the context of a limited number of computers in use, but the legislature did not provide any specific countermeasures against the phenomenon, leaving law enforcement to deal with it within the traditional legal framework.

Earlier studies implied that electronic computer" crime most probably emerged in the fields of military, engineering, science, finance and commerce at the beginning of the 1950s. Nevertheless, the earliest documented computer abuse, which involved the alteration of bank records, occurred in 1958 (Parker 1989, p. 5). The case became the first Federally prosecuted computer crime in the U. S. in 1966, with a time-lag of eight years. It was revealed that a bank employee had utilized the institution's computer to embezzle cents from interest on long-term accounts (ibid.). The financially motivated employee created a criminal precedent.

Within less than two decades, worldwide computer installations increased from four hundred at the beginning of the 1950s to 60,000 at the end of the 1960s (Hamilton 1973, p. 82). Even so, the scarcity of the new machine still attracted potential users to hack, to gain access, and to utilize unauthorized computer time. The term "hacker" in the traditional sense was not regarded as computer crime, but as essentially pertaining to computer security. The rise of the hacker culture can be dated to 1961 when the Massachusetts Institute of Technology acquired the first computer used for commercial time-sharing (Digital Equipment Corporation (DEC), Programme Data Processor-1, 1963).

The expensiveness and rareness of computers necessitated a shared use of these machines to extend their utility as widely as possible, in which the boundary between authorized and unauthorized use was vague. However, at the same time, a security concern originated due to the breach of access control (Association for Computing Machinery Professional Knowledge Programme 1997). The exploited processing ability, loss of computing time and even waste of electricity alarmed computer owners. Notwithstanding, the computer systems were not generally confronted with threats as serious as the phone systems were. In consequence, the U. S. took action to prevent tampering with the phone system (Meinel 2004). Being an early form of hackers, phreakers' intrusion into and interference with the telecommunications system became a kind of punishable offence.

War has been the perpetual inventor in history. Although the apparent causal relation between the Cold War and the ARPANET was not widely acknowledged in available literature, the latter was surely a product to deal with the threats of a "Hot War" against data transmission system. The advantage of this invention was that even if one part of the system was destroyed by war, particularly by nuclear weapons, the system could function in its other parts through rerouting (Okin 2004, particularly, p. 132). The Internet began in the mid-1960s as a programme created by the U. S. Department of Defence to build a decentralized network that would provide a communication between various sectors of the government in the event of nuclear war or an attack on the U. S. (Hafner and Lyon 1998, pp. 10-14). The nature of the Internet determined that it was connected primarily to some important institutions, but was not open to the general users. An intrusion of the networks would

endanger interests that were mainly military and those of advanced science and technology.

At the beginning of this first stage, there was neither cybercrime nor cybercriminal law in the social and legal environment. When the first computer crimes occurred, no law was ready to deal with them (Chen 1990, pp. 71-86; Nelson 1991, pp. 299-321). With the emergence of the cybercriminal phenomenon, the principle of "nullum crimen, nulla poena sine lege" was applied to protect the fundamental rights of the perpetrators from punishment outside the law. Except for the reluctant application of old laws, there was neither a cybercrime prohibited by law nor a law enacted against cybercrime. Lack of punishment reduced the expected cost of the criminals, which were composed thus of moral costs and substantial costs, specifically, the perpetrators' necessary devices and labour in cybercrime. Because there was no cybercrime law, there was neither expected punishment nor the expected cost induced by the expected punishment. Under such circumstances, the probability of conviction equalled zero. The expected utility of the perpetrator almost equalled the utility of a situation in which crime went undetected or unpunished. According to an economic analysis of crime (Becker 1968, pp. 169-217), those who are risk-indifferent are indifferent to detection and conviction. For those who are risk-lovers, cybercrime becomes a new cause, a new chance, a new challenge, and a new type of risk. For those who are risk avoiders, because of the low risk of detection and conviction rate of cybercrime, they transfer from other offences to cybercrime. Therefore, the number of cybercrimes and perpetrators will inevitably increase.

Apart from the gap in legislation when the first cybercrime emerged, law

enforcement had insufficient capacity to deal with it. However, they tried towards imposing punishment through application of existing laws. These provided for a preliminary deterrence on cybercrime, which could be used to deter the potential offenders of existing types of crimes proscribed by existing laws, but was inadequate to deter potential offenders of the types of crimes not proscribed explicitly by law. The principle of legality and the limited possibility of the legislation restrained the coverage of the law and law enforcement, leaving considerable loopholes and having little deterrence on offences that remained untouched by law. As a result, deterrence brought very low expected costs for these perpetrators.

At the same time, existing laws were applied to the limited number of computer crime cases in countries such as the U. S. In filling the legal gap, the passage of computer crime legislation by states lagged behind computer abuses, and did not happen in this period. Furthermore, the debate about computers and personal information only began in the late 1960s (Wood 1982, p. 111). The debate did contribute to providing some forms of deterrence.

6.3 The rise of the law against the increasing number of cybercrimes

Following the first stage, the subsequent two decades form the second stage, which began from the 1970s and lasted to the end of the 1980s, during which along with individuals' and organizations' increasing dependence upon computers, the threats of computer crime increased. The general tendency was that computer crime continued to increase in volume with a change in methods,

while a legal response also began to emerge.

Understanding of the nature of the computer continued developing. In a British case, R. v Wood, the court held that "The computer was used as a calculator, a tool which did not contribute to its own knowledge but merely carried out a sophisticated calculation which cannot have been done manually."[171] It was not a rare situation that even many commentators doubted the acceptability of the computer, predicting only with extreme carefulness that: "The electronic computer would be technology's most successful machine were it not for the difficulty that people have in accepting it." (Hamilton 1973, p. 81) Others already began to long for the "post-industrial society" (Bell 1974), where the computer would not only be broadly used but also be addictively depended on.

Technological thought developed fast in changing the image of the computer in the 1970s, from a bulky mainframe that filled a building to a computer in a desk; and in the 1980s, from a desktop to a host of old and new devices (Mosco 2004, p. 21). The focus of this philosophy is that: "The computer would be growing in power while withdrawing as a presence." (ibid.) The philosophical imagination and the technological development of new intelligent instruments were propelling an information revolution. Comparatively instant and cheap, an e-mail message could be sent from New York to San Francisco in less than a minute for about one dollar, as Fetherolf (1982, pp. 216-217) said. The futurist Castells bore witness to the fact that:

"We are in the middle of a major technological revolution that is transforming our ways of producing, consuming, organizing, living, and dying."

---

171 R. v Wood [1982] 767 Cr. App. Rep. 23.

(Castells 1985, p. 11)

While technology advanced beyond the ability of the average citizens' understanding,[172] the operation of computers remained straightforward and vulnerable to criminal manipulation (Bequai 1979a, p. 107). According to Bequai, computer crimes during this period fell into five key categories, specifically, vandalism, theft of information, theft of services, theft of property, and fraud (1979a, pp. 106-107). Both the merely psychic satisfaction and the pecuniary gains motivated users to practise unauthorized access to the machines, or to information in the machine, hacking for use only being a less guilty act. In fact, before the 1970s, "using" computers without authorization was more excusable because the available computers were still insufficient. Later in the 1980s, more computers were available and it became unnecessary for general users to intrude into others' systems. Therefore, unauthorized "use" of computers no longer provided an excuse and became labelled "abuse" in legal terms.

During this period, there were only some fragmentary reports of computer abuses and accidents. However, the less bulky, low-cost computer attracted an unprecedented number of hackers with various motivations. Computer crime was comparatively new and authorities reacted in a sluggish manner. It was found that the threat of computer crime was pretty relentless. For instance, the average loss of computer crime was dozens or hundreds of times that of conventional crimes, regardless of whether the hackers obtained monetary benefits or psychological satisfaction.

Within this stage, the term "cyberspace," first coined in a fictional work by

---

172 State ex rel. McCleary v. Roberts, 88 Ohio St.3d 365, 2000-Ohio-345.

William Gibson (1984) to describe the environment within which computer hackers constructed a virtual community, became prevalent. In 1978, nevertheless, a perpetrator deprived a bank of 10.2 million dollars in the Rifkin case (Forester 1990, p. 263). In 1982, a group of hackers intruded into a computer with records of cancer patients' radiation treatment, modification of which might threaten the lives of these patients. Murder became realistic with the computer as a tool (Milhorn 2005, p. 59). In 1986, Stoll uncovered an international espionage conspiracy (Longstaff and co-workers 1997, p. 234). These cases expressed again the potential threats of the hackers against property, life, and state security.

On the other hand, the development of computer technology, which was designed for social welfare, also constituted a significant source of threats to the social order. Similarly, the history of technology has been filled with dilemmas of such a kind. For example, primitive weapons may exactly be productive tools and vehicles may be hijacked. What was going to happen –unfortunately- in the field of computer science was that something destructive would be invented. For example, Dan Edwards coined the term "Trojan Horse" in 1972, denoting an apparently benign macro or utility with undocumented side effects, which may be security violating or palpably destructive (Overill 1998). The Trojan horse caused great security anxiety with institutions such as the military (ibid).

Although it is not an exclusive argument, it has been broadly acknowledged that it was in 1984 when Fred Cohen defined a computer virus in his paper (1984). The threat of malicious programmes such as a Trojan Horse, a virus, a worm, and a logic bomb, all came into being during the 1980s, and necessitated the first business of anti-virus in 1988 (F-secure 2005). These

soft offensive and defensive weapons were expected to play their roles in the information warfare in the near future.

The computer network still played a tiny role during this period. As Clarke (1984) pointed out:

"Even for highly developed countries, these [data and computer networks] are still in their infancy, though they undoubtedly represent the wave of the future." (p. 27)

Nevertheless, computer security incidents increased steadily with the development of computer networks. Losses due to computer crime had been incessantly escalating. In 1980, losses from computer fraud and other abuse of computer systems in the U. S. alone were estimated to exceed 300 million dollars (Wood 1982, p. 69). In contrast, although software theft found its way in 1964 (Forester 1990, p. 3), and in the late 1970s, large-scale piracy became common due to the use of the personal computer and packaged software (Forester 1990, p. 4), there have been very few breaches of privacy reported (Wood 1982, pp. 118-119.).

In the early 1970s, according to Sieber (1998), most developed countries introduced laws criminalizing computer crime. More laws and regulations were implemented in more countries in the 1980s. Within this period, all of the Nordic countries had their data-protection laws in place.[173] Countries made every effort to eliminate legal gaps to punish cybercrime. The characteristics of legal countermeasures during this stage were that:

There were merely fragmental computer crimes and fragmental legislations;

---

173 Such as Swedish Data Act 1973, Norwegian Data Registers Act 1978, Danish Freedom of Information Act 1985, Finnish Personal Data File Act (Act 471/1987), and Icelandic Act respecting Systematic Recording of personal Data 1989.

Legislation concerning computer crime was generally concentrated in a developed country;

New crimes such as time theft posed considerable contradictories in the field of law (BloomBecker 1981, pp. 16-17);

Laws were not effective enough (See Dierks 1993, pp. 307-342; see also Rosenblatt 1990, p. 35), and there was a general "lack of deterrence" (Bequai 1978, pp. 5-6).

In short, at the second stage of the development of cybercrime and deterrence, cybercrime was in its growth period, with both the extent of cybercrime and the supply of perpetrators increasing. Although the costs of cybercrimes were continually increasing due to the increasing legislation and law enforcement, they were lower than other well-punished crimes. Thus why rational criminal investors rushed into the new field. Countermeasures against the increasing crimes increased deterrence, which represented an increased probability of detection by new police forces and an increased severity of penalty through new laws. In the development of the struggle between cybercrime and punishment, most types of cybercrimes emerged and to a certain extent were deterred.

6.4 A legal system wrestling with networked adversaries

The pace of cybercrime became faster and faster. The third stage roughly covered the whole of the 1990s, when cybercrime expanded and the relevant legislation was broadly implemented. During this period, personal computers

entered homes and offices throughout the developed world and even in the less-developed countries (Mosco 2004, p. 2). Bill Gates' The Road Ahead (1995), Nicholas Negroponte's Being Digital (1995) all concentrated on building a new world in cyberspace. Tapscott (1996) announced that:

"Today, we are witnessing the early turbulent days of a revolution...A new medium of human communications is emerging, one that may prove able to surpass all previous revolutions...in its impact on our economic and social life." (p. xiii)

Although the information revolution was processing with different styles in countries at a different economic level, the impact of computers on society seemed to be reaching into every aspect of social life (Mosco 2004, p. 18). Alongside the scientists who were hopeful of the new development, the politicians in addition attempted to connect computer communication, economic growth, democracy, and a better environment. As Al Gore said:

"…[W]e will derive robust and sustainable economic progress, strong democracies, better solutions to global and local environmental challenges, improved health care, and…a greater sense of shared stewardship of our small planet." (Gore 2004)

However, since the 1990s, cybercrime had entered a rapid process of globalization. Initially funded by the government, and limited to academic and official uses, the interest in the commercial use of the Internet began to be satisfied from the early 1990s; since then, computer networks have attracted great public attention (Kollock and Smith 1999, p. 3). The U. S. introduced the concept of the National Information Infrastructure (NII) to "unleash an information revolution" (Rowland 1998). With the invention of the WWW,

access to the Internet was available to average users. The growth of the Internet was surprisingly fast. From then on, global computers connected to and users acquiring access to, the Internet were confronted with threats from a globalized cyberspace. Following the last stage, cybercrimes have developed into forms that are more complicated. The cyberspace where perpetrators lived, the virtuality that they wanted, the cable by which they were linked, the knowledge that they had acquired, the tools that they invented, and the platform on which they shared information provided criminals of different degree of sophistication with new incentives.

Personal information could be caught during the transmission process. Personal computers could be attacked during voluntary surfing of the Internet. Web sites could not only be tools by which attacks were carried out, but could also be targets for attacks. According to the statistics by Alldas.de, about 72 web sites were defaced by 47 attackers in 1998, about 1,079 web sites defaced by 430 attackers in 1999 (Li 2003). The General Accounting Office reported 250,000 attacks against the U. S. Department of Defence computers in 1995.[174] These numbers represented different aspects of the situation of risks and threats on the Internet.

Cybercriminals also found their way into electronic communications, such as the e-mail, the abuse of which became an advertising means for underground marketing, or an annoying forum. The large-scale unsolicited e-mail became known as spam (Kelly 2002), which has been converted into one of the side

---

[174] Union Calendar No. 468, the 104th Congress, second Session, House Report 104-861, Federal Government Management: Examining Government Performances as We Near the Next Century Eighteenth Report, by the Committee on Government Reform and Oversight together with Additional and Minority Views, 28 September, 1996.

products of electronic marketing.

Moreover, a series of attacks from malicious programmes happened (Drummond and McClendon 2001), and web sites suffered great threats. The businesses of anti-virus and of the security services continued developing. By 1990, many anti-virus products were introduced from big companies. To some extent, this indicated that the security-induced cost of individual and organizational users had further increased.

The victimized entities began to report enormous losses caused by the infringement of intellectual property. Many web sites, software authors and ordinary Internet users adopted various ways of transferring and exchanging pirated works. The infringement of copyright text, audio, video and multi-media works had entered a stage that seemed impossible for any of the existing authorities to control.

Cybercriminals attacked various private and public targets all over the world, in respect of which some hacking investigations were successful in arresting the perpetrators. In the U. S., the FBI opened 547 cases of "computer intrusion" in 1998, while the number of such cases increased up to 1,154 in 1999 (Freeh 2000). The financial crisis in Asia and a series of bankruptcies of big enterprises also alerted attention to the fact that cybercrime could bring about disasters to the global economy.

Starting from this period, with the rapid rise of the Internet, the influence of the Internet on cybercrime began to be considered in legislation, the contents of which became rich and the range of which was expanded. The gradual formation of international harmonization affected some national legislation. Computer crime and relevant legislation was globalized, expanded

from developed countries to less developed countries and to developing countries. Law enforcement also took a series of measures against cybercrime. For example, in 1990, the U. S. organized a nationwide crackdown on cybercrime, leading to successful arrests, criminal charges, a dramatic show-trial, a number of guilty pleas, and massive confiscations of digital evidence and equipment (Sterling 1994).

From the above analysis, it can be found that at the third stage of development, cybercrime tended to be saturated and the growth rate was thus decreasing. To reach this stage, most types of cybercrimes emerged and been criminalized, the probability of detection had reached a higher level, severity of punishment had reached a higher degree, and most potential users of computers and networks were connected, leaving little space for the undeterred types of cybercrime. The marginal benefits of one more case of cybercrime was going to decrease, while the marginal costs of one more case of cybercrime was going to increase (for general theory about marginal costs and marginal benefits of crime, see Becker 1968; for modern application of this theory, see Cooter and Ulen 2003). Therefore, cybercrime tends was being saturated. At this stage, deterrence continued to increase to a certain extent, until it reached the completeness, specifically, the optimality of marginal utility.

6.5 The equilibrium between cybercrime and deterrence

Although the commencement of the year 2000 witnessed a surprising breakdown in the network economy boom (Mosco 2004, p. 45), the

cybercriminals did not demonstrate any sympathy with the dot coms[175] nor with the stock markets. The fourth stage developed roughly from the year 2000, when cybercrime was becoming routinized, and the legal gap filled.

The large-scale Denial of Service attack against high profile web sites created great panic in society about the Internet infrastructure (Levinson 2002, pp. 524-525). A long list of viruses that were written by people who were in jurisdictions where there was no law against hacking, that were written by means of specific software, which included multiple methods of attacking, that caused billions of dollars of losses, and that disabled anti-virus products, indicated the seriousness of the threat and the necessity for the countermeasures (See Katyal 2001, pp. 1003-1114).

In contrast to these anarchist attacks, the advance-fee fraud induced the victims to transfer money voluntarily to the criminals. The advance-fee fraud, or 419 fraud, which was named after the applicable section of the Nigerian criminal code and was committed in a more organized manner, has victimized people from around the globe.[176] The average Nigeria 419 victim has lost 5,575 dollars, making 419 fraud one of the most costly financial frauds for individuals

---

[175] Dotcom denotes "a commercial company that operates through the Internet." See Daintith (2004), p. 163.

[176] Nigerian Criminal Code, Chapter 38, Section 419 simply provides for the crime and punishment of fraud:

"Any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years.

If the thing is of the value of one thousand naira or upwards, he is liable to imprisonment for seven years.

It is immaterial that the thing is obtained or its delivery is induced through the medium of a contract induced by the false pretence.

The offender cannot be arrested without warrant unless found committing the offence."

(Fager 2004, p. 20).

As to the increase of web sites, attacks against web sites rapidly increased. According to the statistics of Alldas.de, about 4,394 web sites were defaced by 2,255 attackers in 2000, while about 4,797 web sites were defaced by 667 attackers in the first season of 2001 (Li 2003). The defacement of web sites became a significant problem comparable with graffiti street buildings.

The quantity of cybercrime incidents and malevolent attacks has, nevertheless, fallen from year to year since 2001. According to a survey conducted by the CSI and the FBI in 2003, general financial losses totalled, from 530 survey respondents, 201.7 million dollars, a sharp drop from the previous survey total of 455.8 million dollars. In the 2004 survey, overall pecuniary losses totalled, from 494 survey respondents, 141.5 millions dollars (CSI 2004). In 2005, the survey indicated losses, from 639 respondents, that totalled 130.1 million dollars (CSI 2005, p. 14). The reasons for these reduced figures were not clear, but the improved security measures, law enforcement, legislation and international cooperation may all contribute to prevent cybercrime.

Many developed and developing countries have implemented cybercrime laws. From the point of view of International harmonization, the Convention on Cybercrime entered into effect on 1 July 2004. Starting from the 9/11 attacks, a serious international concern about cyber terrorism was brought about the by large-scale distributed denial of service attacks,[177] and it spread among governments, legislatures, law enforcements, and academia.

[177] Distributed denial of service is a form of denial of service launched from many computers in different locations. See Daintith (2004), pp. 159-160.

At the fourth stage, due to the decrease in the marginal utility and increase of the marginal cost of one more crime, and the constant increase in the means of deterrence, total number of cybercrimes has shown a prospect of decrease in so far as the potential perpetrator realizes the fall in the optimality of benefit from cybercrime (for general theory about marginal costs and marginal benefits of crime, see Becker 1968; for modern application of this theory, see Cooter and Ulen 2003. For a study on economic analysis of cybercrime, see Li 2005b). The cybercriminal will, additionally, have to take higher risks than before. It turns out that risk-avoiders will retreat from cybercrime, that those who are risk-neutral and risk-lovers will also discover it less attractive to commit cybercrime than other crimes, and tend to discontinue their adventure. Under such circumstances, the deterrence exercised by legislation and law enforcement can ultimately be recovered.

6.6 Conclusion

During recent decades, society has experienced a fast and frightening increase in both information systems and information transgression. The development of cybercrime follows a route of innovation of the ICT, generations of computers, enlargement of the networks and emergence of anti-security techniques. The faster the speed of information processing is, the broader the network connection covers, the more users are engaged in the information industry, and the more dependent on information modern society becomes, the higher the risks and the more serious the threats people will have

to face. Naturally, the number and gravity of cybercrime will also increase. However, any increase will not be limitless.

The basic summary of the historical scene revolving around cybercriminal phenomena presents us with the reality that the increase of both cybercrime and deterrence remain unbalanced. In a word, people do much, but not enough.

CHAPTER 7 LIABILITY FOR CYBERCRIME

7.1 Introduction

Crime induces a reaction, the liability that people impose on this phenomenon through established forms of law enforced by state agencies. Criminal law is an entity subject to incessant changes, depending upon the competing process of two opposite factors, crime, which represents a socially destructive force, and deterrence, which represents a socially constructive force. Consequently, criminal law is not composed of exactly the same components such as existing offences and punishments between one year and another, though the system remains the same. The change has usually been gradual so that no obvious difference can be perceived except over long intervals of time.

However, present society is undergoing so rapid a change through ICT that an obvious comparison can easily be found. Different roles of information systems in cybercrimes and different motivations of criminals make the phenomenon extremely wide in quantity and diversified in forms. The deterrent effect should be achieved by various liabilities. Criminal liability being certain (Lehtonen 2000a), the previous research on the liability of cybercrime has also focused on justifying the possibility of civil remedies (Drummond and McClendon 2001, Bequai 1983, pp. 225-233).

This chapter will analyse the feasibility of different forms of possible liability for cybercrimes. The feasibility is to be established upon the following considerations, firstly concerning the effectiveness of the liability in eliminating the incentives of the potential perpetrators as mentioned above and elsewhere by many others. Another consideration is that of concentrating on the enhancement of the mechanism of traceback.

7.2 Criminal liability, civil liability and administrative liability

In imposing sanctions on cybercrimes, alternative liabilities may be any of the three kinds: criminal, civil and administrative liability. Criminal liability is the most common choice; importance of civil liability is increasing; while administrative liability has only a limited role in combating cybercrime.

The justification for criminal liability must refer to the reasons for imposing a penalty. Since Jeremy Bentham,[178] criminal science has been built up on the supposition of crime as rational behaviour. People prefer committing crime to behaving legally because the gain from illegal activities is bigger than that from legal activities. Becker (1968) developed the theory from the viewpoint of the economic analysis of crime. Criminals are supposed not only to be rational, but also calculating. Imposition of punishment is to raise the expected costs and diminish the expected benefits of crime. When detection counterbalances the benefits, the potential perpetrator would give up crime. In order for the punishment to deter crime, severity of penalty should be fully taken into

---

[178] The utilitarian philosopher, holding that pleasure is the chief end of life and that the greatest happiness for the greatest number should be the ultimate goal of human beings.

account to supplement the insufficient probability of detection and conviction (see Becker 1968).

These deliberations only give half the answer. The fact is that many other criminals are hardly rational, and are not really calculating, either. So traditional deterrence can work only in the case of rational criminals, but cannot work against irrational criminals.

Punitive liability is based on the proportionate principle, that is, the penalty should equate with the severity of an offence. The complete contents of the proportionate principle include the following aspects: that all offences should be punished, while a non-offence should not be punished; a serious offence should be punished with a severe penalty, while a less serious offence should be punished with a less severe penalty; accomplices in complicity should be punished according to their roles in the offence.

It has been assumed that the purposes of imposing criminal liability fall into two categories, that of special deterrence and that of general deterrence.[179] In the case of cybercrime, criminal liability is definitely the choice that has priority.[180] The effectiveness of deterrence depends on the severity of punishment and the probability of conviction (Becker 1968). The probability of detection and conviction is limited by the characteristics of cybercrime. It is possible to raise the probability of detection, but it requires an increasing investment of both money and human resources on law enforcement (Mermin 1973, pp. 14-20). Even if investment is increased, the probability of detection cannot be 100

---

[179] Claimed by Cesare Beccaria in Crimes and Punishment (1764). See, for example, Levinson (2002), pp. 512-513, for a detailed introduction.

[180] The author wishes to impose a caveat about the view that it is time to abolish punishment and prisons as uncivilized.

percent. In fact, the probability of detection in cybercrime has been very low, due to the preference and ability of both criminals and victims to hide their crimes. Another way to increase deterrence, however, is to aggravate punishment. The severity of punishment is also subject to limitation by recognition of certain factors, of the seriousness of the offence, of humanitarianism, as well as of the cost of punishment, particularly imprisonment. Instead of imprisonment, if a substantial sum of a penal fine were imposed, and the criminal's financial situation could not meet the requirement, the actual enforcement might be impractical. It is, therefore, difficult to say whether fine could act as a complete substitute for imprisonment. In consequence, it may be argued that, the effectiveness of criminal liability is important but limited. At the same time, criminal liability alone does not provide any remedy for the victims, who in many cases suffer more or less losses.

In addition, although criminal law can cover negligent and strict liability, the current laws generally criminalize only intentional cybercrimes. While there is a concern about undercriminalization, critics have also argued that overcriminalization may happen. Besides, it is still disputable as to whether their activities should be criminalized.

It is possible to say that civil liability is a necessary remedy to cover the insufficiency of criminal liability, even though it is designed primarily to provide a remedy for the victims. Civil liability is not a substitute for criminal punishment. If criminals only bear civil liability, the effectiveness of deterrence will mostly be absent. Civil liability thus plays a weaker role in deterrence than criminal liability. However, it has a strong function in providing a remedy for the victims by making the criminals pay. By doing so, civil liability can

compensate at least for a part of the victims' losses, and can reduce the gain of the criminal from cybercrime. If there is a civil liability, potential perpetrators will inevitably consider it more expensive to act illegally. Laws in many countries have imposed civil liability. For example, the U. K. Copyright, Designs and Patents Act 1998 provides civil remedies to compensate victimized intellectual property rights holders and for other copyright offences included in Section 107. In addition, by holding the third parties liable, civil law in many countries allows a victim to recover losses from third parties if their negligent or intentional act has caused the loss (Kenneally 2001, p. 63). In cyberspace, third parties may be the only source of recovery. The direct effect of third party liability is that it creates incentives for the parties to invest in maintaining effective security protection. However, as we mentioned above, the deterrence of civil liability should not be expected to be too effective. Civil liability is confronted with the same problem of the low probability of detection. If the probability is too low, civil liability will also be ineffective.

In order to maximize the effectiveness of the deterrence, criminal liability, civil, and administrative liability should be imposed simultaneously. The criminal should be held to be liable on all three grounds. In addition, other individuals and corporations should be held liable for relevant behaviour in the same case. These should include personnel in charge of management who have abused their duties, intermediaries who have failed to provide reasonable supervision of criminal users and protection for victim users, and manoeuvred third parties who have failed to protect their own systems and failed to prevent their systems from being used in attacks against others.

7.3 Individual liability and corporate liability

The subjects (perpetrators) of cybercrime can have different combining forms: a simple individual, several unorganized individuals, several organized individuals, and a corporately organized form. When only one individual is involved in the case, liability is limited to this person only. When more than one individual are involved in the case, they may form conspiracy, gang, or organized crime ring. In traditional criminal-law theory, these cybercrimes of different organizing structures may still induce individual liability. However, the liability of each individual may be determined by the role that this person has played in the illegal activities, including being a principal, aider and abetter, leader, organizer, etc.

It is possible that cyber conspirators are distributed in different places (cities, provinces or countries), and communicate and commit the crime with the help of the Internet. The trans-territoriality of this kind of crime makes it complicated to investigate and hold the conspirators liable.

When a great number of individuals commit a crime, the opportunity of impunity becomes bigger (Radzinowicz and King 1977, p. 44). Cyber gangsters are not necessarily more organized than other conspirators are. However, they may be more widely dispersed and operating on a larger scale. Hactivists may be classified into this category. At the same time, gangs in the traditional sense can be formed with the help of the Internet.[181] Pure cyber gangs may not only be organized through the network but also commit offences online.

---

181 Eastday, Four Liaoning Cyber Friends Allied Robbing Taxi, Killing Driver and

Organized cybercrime, cyber terrorism, and cyber war are also possible. After the 9/11 attacks, individuals, organizations and governments all over the world became aware of future threats in cybersecurity. Brenner (2002) explored the problem of possible influence of cyberspace on criminal organizational forms. Many commentators have also written and reported about cyber terrorism and cyber war. In cyber terrorism, cybercriminal organizations should be held liable. In cyber war, even a state may be involved in an international offence and be criminally liable.

Corporations are increasingly the actors in the new social structure (Coleman 1990). Individuals are the necessary ingredients of corporations but corporations are different from organized individuals in that the organizing form of the former is subject to a legal character. Corporate liability is disputable even in the framework of traditional criminal law. However, the tendency is that an increasing number of countries adopt the theory and practice of corporate crime. It is natural that corporate cybercrime should also be held liable through criminal-law reform in response to the new criminal phenomena. According to the U. S. Department of Justice (2003),[182] Article 12 of the Convention on Cybercrime and the Explanatory Report paragraphs 124-125 provide that only if a person's act constitutes an offence under traditional principle of corporate liability, may the corporation face criminal, civil or administrative liability. Mere users' actions are excluded from corporate liability. According to the Convention on Cybercrime, corporate liability is established

Burning Corpse, 18 March 2006. Retrieved 15 February 2016, from http://news.eastday.com/eastday/node79841/node79860/node124570/userobject1ai1922624.html

182 U. S. Department of Justice. Frequently Asked Questions and Answers-Council of Europe Convention on Cybercrime, November 2003.

based on the individual or organizational activities of a natural person who holds the power of representation of the legal person, who has an authority to take decisions on behalf of the legal person, or an authority to exercise control within the legal person.[183] Upon ratifying the Convention, individual countries shall have to implement its provisions concerning the liability of legal persons for some of the cybercriminal offences originally absent from their own national law.[184] Besides Internet service providers, there are many other corporations engaged in online activities associated with the relevant obligations. Corporate liability can be of a particular severity, for example, in the U. K., corporate criminal liability can result in penalties on companies and their directors of unrestricted fines and less than two years of imprisonment. The same spirit of the law can well be extended to these corporations and possibly impose liability on them. We now indicate the legal remedy that can be used resolving the underlying problems envisaged earlier. We therefore turn to the remedy of liability for damage.

7.4 Liability based on law and liability based on contract

Before liability for cybercrime is imposed, law or contract might provide obligation or responsibility. The liability comes from a breach of law or contract

---

183 Council of Europe, Article 12.1, Convention on Cybercrime, Budapest, 23 November 2001.

184 HE 153/2006, Detailed Justifications, 1. Contents of the Convention and its Relation to Finland's Legislation, Part II National Measures.

in the form of the commission of a proscribed act or the omission of a prescribed act.

Law prohibits cybercrime. Committing a cybercrime must induce liability. However, the law does not run concurrently with the development of technology. The concern of liability must be widened. According to the principle of legality, the supposed liability does not exist in law. Therefore, legislation should be the basis for liability.

On the other hand, a promise can be made in a contract to create obligations. When one party breaches the obligation, the aggrieved party may be remedied according to contract law. Liability in contract law can create an incentive to maintain a secure critical infrastructure. This kind of obligation can be agreed in the contracts between institutional users and service providers.

However, my research found that individual users are generally excluded from the mechanisms in which the dominant parties are service providers. For example, many service terms drafted and enacted by online enterprises usually include a unilateral disclaimer of warranties and limitation of their liability.

The disclaimer of warranties requires users to understand explicitly and agree to use the service at their sole risk. The enterprise expressly disclaims all warranties of any kind, whether express or implied. The enterprise further states that it makes no warranty that the service will be uninterrupted, timely, secure or error-free; and any errors in the software will be corrected, etc. If users download or obtain by other ways any materials, it is at the users' discretion and risk. The limitation-of-liability clause claims that the enterprise shall not be liable to the users for any direct, indirect, incidental, special, consequential or exemplary damages; unauthorized access to or alteration of

the user's transmissions or data, etc.[185] The basic relationship in these clauses is that service providers make no promise, but make a non-promise. Non-promise results in no obligation of warranty. Non-obligation results in no liability.

7.5 Intentional liability, negligent liability and reckless liability

Current criminal-law countermeasures generally criminalize intentional conducts, whether in the domestic legislations of various countries or in the Convention on Cybercrime. The Convention requires countries to implement domestic laws to criminalize the following unauthorized conducts:

Intentionally accessing information systems (illegal access, Article 2),

Intentionally intercepting information systems (illegal interception, Article 3),

Intentionally interfering with data and systems (data interference, Article 4, and systems interference, Article 5),

Intentionally misusing devices for the purpose of committing any of the offences mentioned above (misuse of devices, Article 6),

Intentionally aiding and abetting the commission of any of the above offences (Article 7).

---

185 See Yahoo!, Terms of Service. Retrieved 15 February 2016, from http://docs.yahoo.com/info/terms/

The Convention leaves countries to make further requirements or reservations, but the subjective aspects are not in the items of the Convention subject to such discretions.

If users fail to secure their own information systems from outside exploitation and cause damage to another user, they should be held liable for the negligence and compensate the victimized party. The prerequisite for this negligent liability is that users do not take sufficient care to protect reasonably their information systems.[186] The factors in judging whether users are taking reasonable care include the amount of information held; the form in which information is retained; the sensitivity of information; the level of risk; the size of the company; and the cost of rendering information systems secure.[187]

Concerning negligent and reckless liability, there are several situations:

1. Laws specifically exclude negligent liability. For example, in U.S.C. 18 §1030 prescribes that negligent design or manufacture of computer hardware, computer software, or firmware are immune from a civil action to obtain compensatory damages and injunctive relief or other equitable relief by any person who suffers damage or loss (The U.S.C. 18 §1030 (g)).

2. Laws criminalizing intentional conduct also involve punishment for some kind of negligent or reckless misconduct. For example, the Section 151b of the Penal Code of Norway criminalized the act of negligently destroying, damaging, or putting out of action any data collection or any installation for some critical sectors, and imposes fines or imprisonment for a term not exceeding one year.

---

186 Bridge Point Communications, Information Security: Corporate and Individual Liability, October 2001, pp 1-2. Retrieved 15 February 2016, from http://www.bridgepoint.com.au/LinkClick.aspx?link=PDF+Docs%2Fliabilitypaper.pdf&tabid=36&mid=376

187 ibid.

The Section 250 of the Norwegian Crimes Amendment Act 2003 prescribes punishment for act of intentionally or recklessly damaging or interfering with computer systems (Section 250). That is to say, the severity of intentional liability and reckless liability are treated equally in the offence of damaging or interfering with computer systems. Section 251 also provides the reckless factors in the offence of making, selling, or distributing or possessing software for committing a crime, "knowing or being reckless as to whether it will be used for the commission of a crime." (Section 251 (1) (b)) Section 252 (1) also prescribes recklessness as a factor in the offence of accessing computer systems without authorization, "every one is liable to imprisonment...who intentionally accesses, directly or indirectly, any computer system without authorization, ...being reckless as to whether or not he or she is authorized to access that computer system." (Section 252 (1)) However, this is hardly to say that Sections 251 and 252 establish reckless liability. Similarly, the 18 U.S.C. §1030 also includes a clause to penalize recklessly-caused damage, but as a result of *intentional* access to a protected computer without authorization (The U.S.C. 18 §1030 (a) (5) (A) (ii)).

3. Legislation proposals, such as the model law of the Commonwealth, taken in reckless liability. The Commonwealth's model law has extended criminal liability to the *mens rea* of offences of interfering with data, interfering with computer systems, and illegal devices so as to include reckless liability.[188] The establishment of negligent liability contributes to forming a close legal framework in combating cybercrime through strengthening the security consciousness of information-systems users, particularly management. To date,

[188] Legal and Constitutional Affairs Division Commonwealth Secretariat, Report on Law and Technology Workshop for the Caribbean, Kingston, Jamaica, November 3-7, 2003, published in January, 2004.

explicit negligent liability for cybercrime is still, however, absent from the international instruments and laws of most countries.

7.6 Direct liability and indirect liability

Direct liability is the liability directly derived from the illegal act that involves information systems. As in the situation where traditional offences are prohibited, the basis for cybercrime liability is the same as for the non-cybercrimes. We are not discussing various theories about what the basis for criminal law is, nevertheless, cybercrime is no different from the older crimes in that old crimes infringe human rights and property rights, and violate the social order. Indirect liability is the liability that is derived from the omission of supervision and management over the activities of the perpetrator or over information systems. The establishment of obligation is the prerequisite for indirect liability. The effective incentive for the responsibility of supervision and management must be ensured by work ethics, rules or disciplines, and civil, administrative, or criminal liability. Kelly (2002) analysed the institutions' liability for e-mail in further education and higher education institutions. He pointed out that e-mails may be regarded as published information originating from the institution and the liability for its publication may attach to the institution. If the institution is held liable, this liability is derived indirectly from the users' act.

7.7 Trespasser's liability, third parties' liability, and victim's liability

Trespassers include a wide range of individuals and corporations: system intruders, virus creators and distributors, illegal web site owners and administrators, authors of illegal contents, illegal service providers, illegal product traders, and so forth. Trespassers' liability includes criminal liability, civil liability and administrative liability for their cybercriminal act.

Third parties include Internet service providers, security publishers, Internet security providers, software vendors, software authors, and system owners. They may also be criminally liable, but in most cases, their liability should be to provide civil remedies for the victims. According to the U. S. Department of Justice (2003),[189] the Convention on Cybercrime does not require the service providers to monitor content to avoid liability. The provisions of the Convention governing aiding and abetting do not naturally apply to the service provider (Article 11, and Explanatory Report paragraph 119). This Convention exempts third parties from liability, but is limited to the Internet service provider as far as Internet content is concerned.

Summing-up the discussion of Icove and co-workers (1995), Drummond and McClenden (2001), Fisk (2002), and others, about third parties' liability, covering ISPs, security providers, software vendors, software authors, and system owners, the situation is that where no liability mechanisms are implemented, they will have insufficient incentive to provide higher standard of products or services. The following Canadian case proved that the absence of liability mechanisms leaves the relevant party unaware of unauthorized access

---

[189] U. S. Department of Justice. Frequently Asked Questions and Answers-Council of Europe Convention on Cybercrime, November 2003.

concerns.

"Several participants in online contests run by the company in question received telephone calls from a person or persons falsely claiming to represent the company. In an internal investigation, the company cannot determine exactly how unauthorized persons had obtained personal information collected from contest entrants, but believed it possible that the computer database in which information was stored may have been compromised. An inspection by an outside firm cannot confirm how or even whether the database had been compromised, but did give rise to several recommendations towards improving the company's informational security. The company has adopted all recommendations and has taken specific measures to physically secure contest participants' personal information from unauthorized access.

At the time of the complaint, the company had no policies for the retention and disposal of personal information. On the advice…the company has also agreed to implement such policies."[190]

The reason for insufficient incentive is mainly that the improvement of quality of products or services is costly, requiring more investment of money, time, and human resources. Liability mechanisms will create incentives to provide products or services on at least a standard level. Products and services containing security defects are at great risks of falling fool of product liability.

However, holding third parties liable is not without risks, because products and services are usually provided subject to contract or licensing agreements, making tort liability inappropriate because the parties have bargained to allocate the risk between them (Perle and co-workers 2000, pp. 10,

---

[190] Finding #52, 2002 CanLII 42357 (P.C.C.).

12). The reasonable starting-point for concluding agreements is that neither of the two parties wants to endure more risk. In general, product or service users may have greater discretion in choosing more guarantees and fewer expenses. Third parties will generally be worse-off. However, third parties will pass on to the users the extra costs in improving the quality and fixing the loopholes. They will raise the prices of their products or services to a higher quality level.

Particularly, there are also some unique aspects of software that make it challenging to apply traditional concepts of liability to free software authors. Free software is also called open source software, which is software that must be distributed with a source code included or easily available, such as by free download from the Internet (Kavanagh 2004, p. 1). As a movement, free software dated from 1984, when Richard Stallman first published the idea that software should be free "as in speech," so that users can review it and change it, as he or she requires to (Kavanagh 2004, p. 2). The term open source dated from 1997, when Eric Raymond, Tim O'Reilley, Bruce Perens and others decided to emphasize the technical and practical advantages of open source software to avoid making the idea less attractive to businesses (Kavanagh 2004, p. 2). Kavanagh (2004) claimed that open source is successful (pp. 19-40), good (pp. 41-52), inadequate (pp. 52-55), more difficult (pp. 56-62), but he mentioned nothing about security. However, the open source licenses usually include a disclaimer of warranty or limitation of liability.[191]

The disclaimer of warranty usually reads as the following:

"…[T]he Original Work is provided under this License on an "AS IS"

[191] Kavanagh (2004) listed licenses of GNU General Public License, Mozilla Public License, and The BSD License. In fact, many other open source licenses are available from the Internet.

BASIS and WITHOUT WARRANTY, either express or implied, including, without limitation, the warranties of non-infringement, merchantability or fitness for a particular purpose. THE ENTIRE RISK AS TO THE QUALITY OF THE ORIGINAL WORK IS WITH YOU…"[192]

The limitation of liability usually includes something of this kind:

"Under no circumstances and under no legal theory, whether in tort (including negligence), contract, or otherwise, shall the Licensor be liable to anyone for any indirect, special, incidental, or consequential damages of any character arising as a result of this License or the use of the Original Work including, without limitation, damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses. This limitation of liability shall not apply to the extent applicable law prohibits such limitation."[193]

Under such circumstances, if we impose liability on authors, it is impossible, because authors get no income to pay the compensation. It is inefficient, because authors will be discouraged from contributing. It is unfair, because users use the software for free and voluntarily. Finally, it is at the users' "entire risk" to use such software, because prior agreement between authors and users distributes this risk to users.

Security (defects) publishers are different from other third parties in that they may have two aspects of gain from the publication, one is that the publication can prevent some harm suffered by the general public, the other is that the publication realizes more economic or other benefits. However, there

---

192 Open Software License ("OSL") version 3.0.
193 ibid.

is a great risk of resulting in users' losses where hackers exploit the publicized loopholes. In addition, users must be expected to invest in improving their security level when they know of the newly publicized loopholes. Whether the publisher should be held liable for his publication, is a question of a nice calculation. What has to be weighed, on the on side, is the gain of users from the stopping of the potential harm and the publisher, too, obtaining a higher confidence value, and on the other side, the losses users suffer from attacks launched to exploit publicised loopholes and the cost of preventing the attacks. In different cases, the cost-effectiveness relationship is different and is hard to make a choice. Finally, as Preston and Lofton (2002) put it, it is a question of whether a specific rule of liability concerning information security publications causes more harm than good, rather than whether an individual publication does (p. 130).

A victim of crime is not always innocent. However, traditional criminal law does not impose punishment on a victim. The notion of culpable victim merely means that the victim induces the offence against him or her. To impose punishment on victim or on the responsible personnel of the victimized institution becomes realistic in white-collar crime and corporate crime. In information systems, victim liability is no longer a taboo. The culpable victim may be punished either due to his or her preceding illegal behaviour or due to his or her failure to prevent the illegal behaviour. In some special cases, laws also impose such a liability on victims. As Sadowsky and co-workers (2003, p. 175) have pointed out, if a site is made inoperable by a denial of service attack, the company may be liable for claims based on breach of contract. Definitely, in this case the victim of the attack also breaches the contract and becomes a liable

party. However, it is necessary to avoid over-criminalization and mis-criminalization. The EU Framework Decision on Attacks against an Information System (12 May 2003) recognized the "need to avoid criminalizing the right-holder and authorized persons." (Preamble (13)).

7.8 Domestic liability, trans-national liability, and international liability

Some kinds of cybercrimes are usually aimed at domestic targets, though perpetrator and victim are not necessarily the same jurisdiction. The general principle of jurisdiction can be applied to deal with such cases. Criminal justice assistance is also necessary in investigation and prosecution.

The trans-border nature of the Internet often enables trans-national cybercrimes: an offence being carried out from different countries; an offence targeting victims in different countries; or an offence targeting a floating victim who travels through states A, B, C, etc. All these cases are brought about by the trans-border information flow. In the last few years, people have compared information systems with a superhighway. Wherever information can reach, there information systems can facilitate cybercrime. Relationships between offenders, victims, and intermediaries that link them are all connected into this system, enjoying the wealth of information and taking potential risks. It is natural that the trans-border liability will be prevalent.

Cybercrime of an international nature, such as cyber terrorism and cyber warfare, is comparable to traditional international crimes. Universal jurisdiction should be applied in such cases. However, this is still a theoretical supposition.

7.9 Offensive liability and defensive liability

Offensive liability is the liability for the offensive act. The person who is liable for his or her offensive act is the perpetrator of cybercrime. Defensive liability is the liability for omission of the defensive act. Cybercrime does not always result in defensive liability. However, if there is a legal obligation upon the parties whose systems are targeted or exploited, victimized or exploited parties may also be liable for the omission of an obligation. In content-related cybercrimes and denial-of-services attacks, the content-service providers and compromised computers are in a defensive status and potential liability falls into the context of defensive liability. Traditionally, subjects in a defensive status are only liable when there is a legal basis for the logic of "failing to prevent a crime is to cause it," and where, usually, big organizations become significant targets of public complaint about crime (Sherman 1995, pp. 102-113). In the network environment, two contrary tendencies exist in the meantime. One is the pressure of imposing suitable obligations for the prevention of cybercrime in big online enterprises, the other is that these enterprises have sufficient power to resist this kind of pressure. Therefore, if defensive liability comes into being some day, it would hardly be in a short period of time.

7.10 Punitive liability, exemplary liability and compensatory liability

Punitive liability is the liability primarily for punishing the offender and deterring further offences. The punishments provided in criminal law, such as imprisonment and fine, are designed to serve this function. All of the offences, including cybercrime, are treated similarly in criminal law. Although the purpose of modern criminal law is deterrence, the innate nature of the penalty is to punish the criminal. This nature has never been changed by the development of a set of modernized terminology in criminal law. The terminology functions mostly in adjusting the principles to changing social needs. Consequently, the punitive nature of criminal law has shown a reduction in the severity of its linguistic expressions, and less concrete structures. However, when we discuss criminal law, we are straightforwardly relating the person to the artificial unhappiness of the punishment, which is the consequence of the inherent liability of committing a crime.

Exemplary liability is liability for alerting the perpetrator, containing both punishment and compensation. Exemplary compensation is a kind of liability that imposes monetary damages greater than the actual losses. Due to the low probability of detection of cybercrimes, punishment should be severe enough to deter them. The exemplary liability may be a useful way of increasing the severity of punishment. The reason why exemplary liability is supposed to be effective is that socialized individuals are morally responsible and psychologically correctable. Exemplary liability symbolizes cybercrime as a moral wrong and an unfair psychological gain. What is a moral wrong should be

publicly reprimanded, while deprivation should be the fate of what is unfairly gained. Beyond reprimand and deprivation, exemplary liability is designed to prevent future wrongdoings.

Compensatory liability is liability primarily for compensating losses of the victim from cybercrime. Compensation is generally meant to match the losses of the victim. Such compensation falls into the field of civil liability. Because cybercrime usually causes great losses for the victims, the compensation helps the victim to recover the whole or part of the losses. The revelation of a personal message or trade secret may be a fateful incident for the reputation of an individual or business of an enterprise. While compensation for a sum of millions of dollars cannot be afforded by most hackers, smaller sums of compensation are quite realistic. The necessity and possibility of compensatory liability for some victims of cybercrime is justified as a complementary remedy.

7.11 Conclusion

In the case of cybercrimes, the losses from the criminal action are mainly pecuniary, while the damages are non-substantial. In addition, there is usually an involvement of multiple parties in the cybercrimes and thus the identification of subjects becomes difficult. This necessitates the establishment of a multi-layer liability system of multiple subjects. Moreover, the damage from cybercrimes is great, while the detection probability and rate of conviction are both low. This demands the imposition of heavier sanctions than in the case of crimes with a higher detection probability.

Liability can only be effective when it discourages criminals, creating an incentive for security. If there is no incentive, even if there is liability, there should be no liability, because this kind of liability is not cost-effective and inefficient. On the other hand, the establishment of liability should be based on creating incentives for the subjects, to prevent those who distribute software which is vulnerable to hacking, those who access the Internet with the possibility of being exploited by attackers, and those who provide security services that are insecure, and so on.

However, the law should not be there to hold all those responsible liable when the breach of responsibility is expressed in the form of a crime, but to impose liability, as necessary, on those whose activities reasonably cause the effect according to strict legal principles. The above discussion is to demonstrate the possibility of liability forms rather than to create liability for any user of information systems.

Liability is not in the air, but on the ground. Liability should be fixed by legislation, as has been stated in this chapter. However, liability also should be established in jurisdiction, as we will see in the next chapter.

CHAPTER 8 CYBERJURISDICTION

8.1 Introduction

Unless jurisdiction can be exercised over cybercrime, no liability can be imposed on the perpetrator. Jurisdiction is not a problem emerging only in issues associated with information systems (Westby 2003, p. 41). However, it is becoming significant in the digitalized environment. Crime is undergoing a process of globalization (Findlay 1999, Lehtonen 2000b); cybercrime particularly is in principle borderless. Smith, Grabosky and Urbas (2004, pp. 48-49) have summarized four challenges that the trans-national dimension of cybercrime poses for prosecutors: to establish the criminal jurisdiction of an act in question, to collect adequate evidence to activate the law, to identify the criminal and to decide his or her physical location, and to decide either local jurisdiction or extradition.

Actually, many elements have significant functions in deciding which court has power to exercise jurisdiction over a criminal case. The Internet poses the great challenge to the traditional practice of exercising jurisdiction. The trans-border nature of information systems makes the boundary of criminal jurisdiction more ambiguous. Technically, the perpetrator can give a command

to a computer in State A to modify data physically stored in a medium located in State B, without the knowledge of the actual location of the data. The modified data may produce a harmful effect in State B after crossing communications networks located in several other countries. Based on the traditional theory of criminal jurisdiction, many countries can claim jurisdiction over the case based on the acts of modifying the data, the transmitting of modified data, and the emergence of harmful effects. It is difficult to determine the geographical location and thus the jurisdiction.

In addition, the uncertainty in cyberspace complicates the traditional criminal jurisdiction. In the latter, the nationality of the perpetrator, the location of the act and the effect can be the basis for the criminal jurisdiction because of their link to a substantial location of a certain jurisdiction. In cyberspace, however, the link between these factors and substantial location becomes uncertain. We cannot find the residence and tangible property; determine the nationality of the actor, and the exact location of a remote logging on, but only the existence of the actor and the detailed contents of the criminal act. In sum, the traditional criminal jurisdiction should now be globalized (Berman, 2002).

8.2 The legal basis for cybercriminal jurisdiction

Criminal jurisdiction means the power of a state to prosecute and punish the criminal. In terms of international law, it is the foundation for dividing the power between countries over a criminal justice that involves international factors (Zhao 1994, p. 116). The established principles of criminal jurisdiction

over international crime include the principle of territorial jurisdiction, the principle of personal jurisdiction, the principle of protective jurisdiction, and the principle of universal jurisdiction. The former three principles are also effective in domestic criminal law, and the last principle is unique in international criminal law.

"Sovereignty accorded each state supreme, comprehensive and exclusive rule over its territorial jurisdiction." (Linklater 2000, p. 1504) Under this principle, the criminal is subject to punishment by the state where the crime was committed, without considering the nationality of the criminal (Van Dervort 1998, p. 254). Law shall apply to a crime committed in the state where the law is enacted.[194] Vessel and aircraft are generally deemed to be the extension of the territory of a sovereign state, whose flag they fly regardless of where the vessel or aircraft are located, even if the vessel was on the high seas or in foreign territory, or even if in the territory not belonging to any state or the aircraft was in or over such territory.[195] According to this principle, determination of the location of cybercrime is the basis on which to decide whether a state has jurisdiction. The act and effect of cybercrime usually involve several locations in different states. If every state claims criminal jurisdiction over the same offence, jurisdictional conflict is inevitable.

At the same time, the determination of the location of cybercrime is more difficult in other aspects. The focus of the disputes resolves around the places which can be identified as the locations of an offence. Traditional theory adopted the places where the act of the offence was committed and where the

---

194 See, for example, Penal Code of Finland (39/1889), Chapter 1, Section 1. The English translation was made by Ministry of Justice, Finland, as an unofficial translation.
195 See, for example, ibid, Chapter 1, Section 2.

harmful effect of the offence happened.[196] In cybercrime, the act can be carried out in a place thousands of kilometres from the place of its actual effect. However, the location where the computer was in operation is publicly regarded as the location of the act. What is still disputable is whether the places where the transmitted data pass (that is, the networks) and arrive (that is, terminals) and where the web pages are deposited (generally, servers) can be regarded as the location of an offence.

The negative answer to this question was partly given in Directive 95/46/EC, Article 4.1(c) provides that if "equipment is used only for purpose of transfer through the territory of the Community," national provisions will not be applied. In fact, this provision has almost unanimously been provided in the laws of member states.[197]

The principle of nationality is designed to protect the legal rights of domestic or local citizens, and prevent an unjust trial of domestic or local citizens by other states or regions: the criminal is subject to punishment by the state, to which the criminal's nationality belongs (Van Dervort 1998, p. 261). The principle of active nationality applies to cases in which the offenders are

---

[196] See for example, ibid, Chapter 1, Section 10, providing that "An offence is deemed to have been committed both where the criminal act was committed and where the consequence contained in the statutory definition of the offence became apparent. An offence of omission is deemed to have been committed both where the offender should have acted and where the consequence contained in the statutory definition of the offence became apparent." In the cases of attempt and complicity, the location where the offence might have been completed or the consequence might have appeared, or the consequence that the offender thought would appear, or the act of complicity might have been committed, shall apply the Finnish law.

[197] See Danish Act on Processing of Personal Data (Act No. 429 of 31 March 2000), Part 3; Finnish Personal data Act (523/1999), Section 4; Icelandic Act on Protection of Individuals with regard to Processing of Personal Data, No. 77/2000, Section 6; Norwegian Act of 14 April 2000 No. 31 Relating to the Processing of Personal Data (Personal Data Act), Section 4; and Swedish Personal Data Act (1998:204), Section 4.

citizens of the state, while the principle of passive nationality applies to cases in which the victims are citizens of the state.[198] However, because offences covered by this principle usually happen outside the state or region, conflicts often appear with the states or regions which claim jurisdiction according to the principle of territory, and result in double jeopardy. Finally, this principle is only applied in grave offence, for example, spreading child pornography and other illegal information. The principle of nationality is designed to supplement the insufficiency of the principle of territorial jurisdiction but not to impose any limit on it. On the contrary, the mere application of the principle of nationality is usually not enough for a state to exercise jurisdiction over events in its territory. Sometimes laws provide explicit clarification of this situation. For example, Section 9 (1) of the U. K. Computer Misuse Act 1990 prescribes that to establish jurisdiction over the offence does not depend on the citizenship of the accused.

The principle of protection is primarily applied to foreigners or stateless persons who commit an offence endangering the state's interests abroad; the victimized state has the power to prosecute or try the case.[199] According to this principle, the state has power to take the necessary measures against the offence which breaches the state's interests. Any online activities have a global nature, which causes many obstacles to applying the principle of protection. On the one hand, the after-effect of cybercrime usually involves many states. If every

198 See for example, Penal Code of Finland (39/1889), Chapter 1, Sections 6 and 5.
199 Zhang (1999), p. 79. For example, the Penal Code of Finland provides that "Finnish law shall apply to an offence committed outside of Finland that has been directed at Finland. An offence is deemed to have been directed at Finland if it is an offence of treason or high treason, if the act has otherwise seriously violated or endangered the national, military or economic rights or interests of Finland, or if it has been directed at a Finnish authority." Chapter 1, Section 3.

state claims criminal jurisdiction, it will definitely cause a jurisdictional chaos. On the other hand, if the cybercrime prescribed in one state is not criminalized in other states, it is unreasonable for this state to exercise jurisdiction. No state is likely to exercise jurisdiction over cybercrime merely according to the principle of protection.

The purpose of the principle of universal jurisdiction is the establishment of consensus on criminal jurisdiction between states to prevent crime effectively and to combat crime under the framework of an international law based on international treaties containing penal provisions, and provided by each country's domestic law.[200] Macedo (2004, p. 9) defined the universal jurisdiction as

"[T]he principle that certain crimes are so heinous, and so universally recognized and abhorred, that a state is entitled or even obliged to undertake legal proceedings without regard to where the crime was committed or the nationality of the perpetrators or the victims. It applies to the most serious crimes under international law: slavery, war crimes, crimes against humanity, torture, and some others."

Because the criminal act and effect relating to the principle of universal jurisdiction usually take place outside the territory of a state, it is by this very nature a matter of a trans-territorial jurisdiction. The global nature of online activities facilitates a cybercrime endangering global targets. However, as to

[200] For example, the Penal Code of Finland provides that " Finnish law shall apply to an offence committed outside of Finland where the punishability of the act, regardless of the law of the place of commission, is based on an international agreement binding on Finland or on another statute or regulation internationally binding on Finland (international offence). Further provisions on the application of this section shall be issued by Decree." Chapter 1, Section 7.

whether the principle of universal jurisdiction can be applied to cybercrimes that has a severe impact on global targets, there has not been relative agreement. The application of universal criminal jurisdiction is primarily based on the nature and gravity of cybercrime. For instance, if there is cyber war crime, piracy, terrorism and so forth, the principle of universal jurisdiction should be applied. As with traditional international offences, the application of universal jurisdiction over cybercrime must be based on explicit provisions in international agreements. Each state cannot apply universal jurisdiction merely according to the domestic law (Bossard 1997, p. 111).

In traditional law, the ownership over land extends to the sky over the land. A state's jurisdiction has the similar pattern, covering surface, underground and airspace, but not outer space.[201] At present, we cannot help asking: does he who owns the soil, own the network? However, we have seen that individuals and institutions can only own the physical materials *of* the networks, but are not able to control the activities *on* the networks. Jurisdiction over uncontrollable "space" has no realistic basis. Physical and spiritual fences in a traditional sense cannot be valid in the networked environment. Furthermore, we must compare offences in cyberspace with those in watercrafts and aircrafts, which are called floating territory. A state has the power to exercise jurisdiction over offences occurring in watercrafts and aircrafts that are registered in the state. Cyberspace is not the same as floating territory in that what extends in cyberspace is not the state's material entity, but is composed of abstract information flows, the

[201] Outer space refers to the space located outside the Earth's atmosphere. See Summers (2003), p. 1168. However, because of its political sensitivity a solution to the definition/delimitation problem cannot be reached on an international level and the issue is still under dispute. See Van Traa-Engelman (1993), p. 47.

owners of which are difficult to determine or are distributed in many different territories. The conception of floating territory cannot form the basis for jurisdiction. Comparable cases also include, for example, the language in which information is compiled. If it is the rule that the language, in which an offensive message is written, is the official language of a state, which thus has the power to exercise jurisdiction, the situation will become even worse. Therefore, both the information flow and language cannot be the basis for jurisdiction. Many other nexuses have a similar nature. It is advisable for a set of new game rules to be implemented in cyberspace.

8.3 "Separate" or "international" jurisdiction?

In the mid-1990s when the Internet was opened to access for commercial use and grew unprecedentedly, commentators advocated that cyberspace should be treated as a separate jurisdiction (For example, Johnson and Post 1996, p. 1367; Oberding and Norderhaug 1996). The theory argues that online communities have maintained community norms and have the ability to create and enforce rights and responsibilities (Oberding and Norderhaug 1996).

In recognizing that cyberspace has its own organizational form, value standard, and rules, separate from those of the government, and that it maintains its own organs of power, the theory advocates that jurisdiction outside cyberspace should be denied. The theory emphasizes the novelty and independence of cyberspace, holding a sceptical attitude towards the power of real-life states, and worrying that the intervention of state power will hurt the

freedom of cyberspace.

Nevertheless, the claim completely confuses two kinds of different powers, specifically, the power of ISPs to establish business ethics and technical standards, and the state power to enact law and exercise jurisdiction. Although business ethics and technical standard to a certain extent may influence law, they can never replace law. Similarly, self-regulation can never be a substitute for the public power of law. Cyberspace should not be beyond the jurisdiction of the courts, and law should be used to protect the liberal development of cyberspace. The fundamental question is how to syncretize the two aspects, and protect the development of cyberspace.

In order to solve the issue of cyberspace jurisdiction, some scholars, represented primarily by Darrel Menthe (1998), put forward the theory of a fourth international space, which is based on the assumption that cyberspace was a new space, but comparable to the *mare liberum*,[202] outer space and the Antarctica.[203] Based on comparison and analogy, Menthe (1998, pp. 101-103) drew the conclusion that cyberspace ought also to accept the implicit international customs, that is, the customs similar to those dominating the other three international spaces, and thus the problem of judicial jurisdiction would be solved by enacting a corresponding regime-specific treaty. He asserted that

---

202 The Latin phrase represents "free sea", a sea open to navigation by ships of all nations. Dutch jurist Hugo Grotius published a treatise "Mare Liberum" in 1609 challenging the right of any nation to claim part of the open sea exclusively as its own. The title translates as "The Free Sea". See McKenna (2003b), p. 225.

203 Territorial claims in Antarctica have been made by the United Kingdom in 1908, New Zealand in 1923, France in 1924, Australia in 1933, Norway in 1939, Chile in 1940, Argentina in 1943 (U. S. Congress, Office of Technology Assessment, September 1989, p. 41). The U. S. and Russia have made no territorial claims and do not recognize the claims of others, though they reserved their rights to assert claims in the continent (ibid., p. 43).

four international regions such as Antarctic, outer space, the high seas, and cyberspace, share the similar characteristics of the lack of territorial jurisdiction, and thus nationality is and should be the primary principle for establishing jurisdiction (Menthe 1998, p. 70).

This theory may have its advantage in solving the cases involving a single criminal and a single victim, or a single criminal and multiple victims. However, there are two points requiring special consideration in dealing with cyberspace. Cyberspace has similarities to the three traditional international spaces in that there has not been a unique state endowed with complete jurisdiction over these spaces. Nevertheless, cyberspace also has its differences from the traditional international spaces. The status of the traditional international spaces has been established by international agreements, while cyberspace is an emerging space without a consensus on its status. In cyberspace, there are relevant territorialities located in several relevant countries, such as where the nationality of a person or several persons belongs, where the web site is registered, where the server is set up or rented, where the victims are distributed, and so on. Traditional international spaces are spaces themselves, involving no other territoriality. In addition, traditional international spaces are beyond sovereignty, while cyberspace is rooted in sovereignty. The only problem is that jurisdictions may be extremely competing between countries. However, merely to avoid competing jurisdictions should not be the ground for establishing nationality as the unique basis for an international rule on jurisdiction over cyberspace. At the same time, even if nationality has been established as an internationally accepted basis for jurisdiction over cyberspace, the "indefinitely competing jurisdictions" cannot yet be avoided, provided that

cybercrime is an organized distributed denial of service attack. In cases involving multiple criminals and multiple victims, the theory of a fourth international space is completely unadoptable. It is hardly strange that these suggestions did not receive any positive reflection from any legislature (Zeviar-Geese 2001; Wober, Frew and Hitz 2002, p. 203).

8.4 The specific space—the determination of the location of conduct

Compared with traditional criminal cases, cybercrime cases have both a common characters and differences that exert an influence on the application of jurisdiction. A number of studies have been targeted on cyberjurisdiction, either civil, criminal, or comprehensive, for example, Biegel (1996), Johnson and Post (1996), Menthe (1998), Post (1996), Jew (1999), Zeviar-Geese (2001), Smolen and Downing (2002), August (2002), Brenner and Koops (2004), etc. The current situation is more complicated than when the problem first emerged before the academic vision, with more possible alternatives for answering the question.

According to the traditional theory of criminal law, if either criminal act or harmful effect happens on national territory, the crime can be regarded as happening in that country. The jurisdiction of the conventional courts is geographically based, with the rule incorporating a notion of territoriality (Jew 1999). When this theory was established, the early criminal law was rarely confronted with the situation of a geographical separation of act and effect. Internet communications are geographically independent. Information is not

limited to one place, but is distributed concurrently globally (Police Commissioners' Conference Electronic Crime Working Party 2000, pp. 25-28; Rees 2000, pp. 16-19). The geographical separation of act and effect on cybercrime is becoming more common.

There does exist a form coinciding with the traditional criminal act. However, due to the spaceless nature of the network environment, attacking targets located in countries other than the one where the perpetrators hold the nationality, where they reside, or where they launch the attack, may easily be realized (Smolen and Downing 2002, p. 2). Add furthermore, the formation of criminal conspiracy, the transmission of criminal command, the transfer of criminal data, and the spread of malicious programmes can all pass any regions or countries that are connected via the Internet. As Lessig (1996, p. 1404) pointed out: online events are taking place "everywhere if anywhere, and hence no place in particular."

Traditional jurisdiction by territoriality has been determined by the place where the offence is committed. The commission place of crime is the basis for determining whether a country holds criminal jurisdiction. We have already recognized the universality of cybercrime: where there is a computer connected to the networks, there is a possibility of being abused. The problem is that millions of computers and more than a billion of Internet users form a dynamic space. The borders between abuse and use, defence and offence, criminal and victim, are not clearly divided before they are defined within a jurisdiction. Computers and networks are value-neutral while users have a different value orientation and are subject to different legal constraints. When there is no applicable law, there will be no difference between crime and

innocence. Cyberspace is a territory with law and order over which no one single government can exercise control, and for which no two governments can cooperate. In the traditional mode, an offence has been easily linked to a place. However, in the Internet environment, as Lessig said, we can regard a crime scene as: "everywhere if anywhere," where the jurisdiction conflicts are inevitable on the one hand; yet are "nowhere," since the jurisdiction gap exists on the other hand. Therefore, the determination of the location of an act becomes more complex and more costly than ever before.

The fact is that jurisdiction based on the location of the act is the most convenient way for evidence collection. According to traditional criminal law, the location of the act includes the location where the act started and where the effect occurs. Any traditional location is connected with an address, which is the physical existence of a particular space. An address on the Internet, however, is not the same as that in the traditional sense. For example, an e-mail address is possibly "an archive server, a list of people, even someone's pocket pager," rather than a human being (Kehoe 1993, p. 9). Therefore, there is no address at all in cyberspace.

8.5 The specific player—the determination of the location of the person

Internet communications enable people to do far more things than clicking the mouse without our physical presence in the place where the effect will happen. The determination of an online user's location is difficult, if not

impossible. Cybercriminals tend to conceal their conduct, identity, and location. The complexities of the relationship between offenders and victims form a more remarkable scenario of international cooperation (Smolen and Downing 2002, pp. 13-14).

Not in all cybercrime cases can jurisdiction be determined by the location of the person, particularly when the investigator has no way of tracing back to the starting-point of the offence when the offender is located in a foreign country that does not have a law criminalizing cybercrime, or has such a law but without an extradition agreement between the two countries. Under such circumstances, the offender has the highest possibility of escaping criminal and other liabilities.

Nationality is not a highly physical way of determining the location of a person. Nationality, nevertheless, has a direct link with a country. Traditional jurisdiction by nationality relies on the nationality of the criminal or the victim, that is to say, active nationality and passive nationality separately. In the Internet environment, both criminals and victims involved in a single offence can be multiple and wide distributed. In some successfully prosecuted cybercrime cases, nationality has, indeed, been used as the basis for jurisdiction.

One of the examples of active nationality is New York v. World Interactive Gaming Corp.,[204] where a New York court denied the claim that the gambling on the Antigua-based web site took place in Antigua, where it was lawful, and the court prohibited the New York owner from doing business with

---

204 People of New York v. World Interactive Gaming Corp., 185 Misc. 2d 852, 714 N.Y.S.2d 844 (N.Y. County Sup. Ct. 1999).

New York residents.[205]

The typical example of passive nationality is that the State of Minnesota in the U. S. seeks to enforce its own domestic legislation against out-of-state Internet users (Jew 1999). The Minnesota Attorney General filed a series of lawsuits against out-of-state users in relation with online conducts that were supposedly damaging to Minnesota residents (Fulford 1993, Cl).

Jurisdiction based on passive nationality facilitates the jurisdiction based on the location where the victimized target is situated. The prerequisites for this jurisdiction are first the coordination of the authorities in the location of the act or nationality, and second the mechanism of extradition. In United States v. Thomas (1996), Robert Thomas and his wife Carleen Thomas in California operated the Amateur Action Computer Bulletin-board System ("AABBS"), transferring pornographic pictures to paid users, with advertisements soliciting users to purchase videos. "Its features included e-mail, chat lines, public messages, and files that members could access, transfer, and download to their own computers and printers."[206] Beyond receipt of a complaint about the AABBS from a resident of the Western District of Tennessee, Agent David Dirmeyer, the U. S. Postal Inspector applied to become a user by nickname, and downloaded several "gif" files as evidence. With this evidence, Dirmeyer indicted the accused for breaching the laws of this state and the U. S. Federal Obscenity Law in the Tennessee Federal Court. The court held that although the accused stored their materials in the computer at home, freely downloaded by the users, and did not breach the law of California, these materials were

[205] Supreme Court of the State of New York, County of New York: Commercial Part 53, Index No. 404428/98.
[206] United States v. Thomas (1996 FED App. 0032P (Sixth Circuit))

found in Tennessee and the couple were convicted according to the laws of Tennessee.[207]

In a broader sense, some newly-developed theories can be regarded as the expansion of the nationality principle, such as the theory of server jurisdiction, the theory of the uploader and downloader jurisdiction, both mentioned in Menthe (1998). The theory of server jurisdiction has its advantages in identifying the location of the server, that is, the registration place. The disadvantage is that the offensive servers may possibly be registered in a country where the law legalizes such activities, while the services it provides may be accessed from all over the world. Then the jurisdiction stops at the state boundaries. In the case of a server as a criminal target, the principle is essentially a jurisdictional variance by passive nationality. The theory of the uploader and downloader jurisdiction is slightly different from a jurisdiction by nationality in that if the offender from state A travels to state B and launches attacks against the targets in, say, states C, D, E... Then, state A is where she or he holds a separate nationality, state B is where she or he commits the offence, and states C, D, E... are where the effects of her or his offence take place. Thus, the theory is in fact a variety of jurisdiction by passive nationality as well.

8.6 Liability-based cybercriminal jurisdiction

The establishment of a nexus for jurisdiction should be based on the existence of liability. Jurisdiction over cybercrime should be built on the most

[207] ibid.

direct link with the liable subject. The location of the act has most direct link with the perpetrator. Therefore, in most situations, jurisdiction is established by the place where the offence is committed, without any exception for cybercrime. Although the process of the criminal act may involve different locations at the same time or at different stages, there is still a place where the perpetrator sends the most direct command, which may be an input from a keyboard, clicked with a mouse, both from a fixed terminal or from a mobile terminal. The location of the terminal is where the criminal most probably appears in person.

The prerequisite for jurisdiction is the existence of liability. It is liability rather than the person or crime that is the basis for jurisdiction. Where there is no liability, there is no jurisdiction. When our discussion resolves around jurisdiction, we are in fact caring about the power to hold the criminal liable. The above-mentioned function of the most direct link indicates that to establish jurisdiction, liability should be identified in the exact location. In traditional criminal-law theory, the principle has already been established that criminal liability starts from the beginning of the act, lasts during the process of the offence, and ends with the occurring of the effect. If the location where the offence begins, proceeds, and ends are different, then the authorities of all the three locations may have jurisdictional power. In addition, emphasis on the traditional theory is placed on the location where the act begins and ends.

In cases of cybercrimes, the separation of the three categories of locations is obviously common. However, the most suitable jurisdiction should be established in the locations where the act is committed or the effect happens. The locations where the cybercrime may "pass by," but does not have an influence on the local interests should not establish jurisdiction, because there is

no existence of liability in such locations. The claim that a server or a web site should be the unique nexus for jurisdiction in cyberspace is not acceptable. If there is no liability for breaching local interests, jurisdiction can only be established according to the principle of universal jurisdiction. Locations of servers or web sites are not necessarily the place where the criminal act begins with a command or ends with an effect. They may be a nexus in some cases, but not the only nexus in all cybercrimes. For example, an individual in State A publishes a message on a web page deposited in a server in State B in order to defame another individual in State C. The calumniator uses the native language that few understand in State B, and few retrieve the massage there. That language may be understood in State C where the victim resides. Apparently, State A and State B should hold the perpetrator liable, but not State B, which is only a place where the message is deposited. However, if the residents in State B can also understand the language of State A, the situation will change, because the effect of defamation also happens in State B. Then State B can establish jurisdiction, even though neither the criminal nor the victim resides there.

The prerequisite for liability is the existence of both act and actor. Criminal liability means that the actor is liable for his or her act. The most convenient situation for exercising jurisdiction is that the actor acts in the same place where he or she resides permanently. We suppose once it was unnecessary to distinguish territoriality from nationality. In the information age, what is common is that both the actor and the act are dynamic, and that even the tools of crime are also the wireless and mobile phone. Yet, the actor and his or her act are necessarily connected with a certain space. For example, an

individual uses a mobile terminal in State A to send a command to a fixed terminal located in State B, the terminal in State B then transmits the command through several nodes separately in different states before it arrives a terminal in State Z, and the terminal in State Z makes the last command and activates hundreds of thousands of terminals located all over in the world to launch a distributed denial of services attack towards a target in Finland. There is no sense in the node states and states where the terminals are located to claiming jurisdiction. However, State A and Finland may have the better reason to hold the individual liable.

Jurisdiction is no more than jurisdiction over the person and over the event. It is a combination of jurisdiction over a liable person and over a liable event. Nevertheless, it is also possible to establish jurisdiction over data packets. When cybercrime involves fraud, embezzlement, illegal sales of drugs, weapons, pornography, and the trafficking of persons, there must somewhere be a location where the substances and victimized human beings are. In addition, supposing that cyber wars or cyber terrorist attacks occur, and the perpetrator has breached international criminal law, then universal jurisdiction may play its role. Any states that have joined the agreement should hold the perpetrator liable. In fact, many new theories on jurisdiction deal with the locations in which these packets are created, sent, transmitted, processed, deposited, or reached. Due to the digital and fluid nature of packets, it is possible, but it is unreasonable to establish jurisdiction over the packets as the only nexus which proves the perpetrator liable.

To meet the requirement for protecting the victims, a jurisdiction is also established which is focused on the victims. However, it is still jurisdiction over

the liable person and liable act. It is meaningless to locate the victim merely. Jurisdiction according to passive nationality is based on the jurisdiction over the criminal. However, it has more meaning in cases of cybercrimes when extraditing multiple criminals to the domestic state of the victim. If cybercrime is an organized attack in which criminals are distributed throughout many states, and in which victims are also located in many countries, jurisdiction according to passive nationality is invalid, and so are jurisdictions according to active nationality and territoriality. No old and new theory is suitable for dealing with cases of this kind. States must negotiate to coordinate their actions. Only if universal jurisdiction is available in these cases can the states reach a consensus to hold these hackers liable, by prosecuting them in one state.

Wherever the starting-point is, the establishment of jurisdiction should be based on the liable person and the liable act. Without these two aspects, there is no liability, and thus no necessity for jurisdiction. If the servers, web sites, and even owners of cables are not directly involved in the offence, they should be immune from criminal liability. For example, if they are abused, exploited, or manoeuvred, they are innocent. Only when they are directly involved in the case should they be liable for the offence, for example, only if the web site itself is designed to spread malicious programmes should the owner be liable.

However, the ultimate bearer of liability is the criminal but not the crime. The purpose of jurisdiction is to hold the criminal liable. If the link between liability and the bearer of the liability cannot be established, jurisdiction is valueless. Those who have claimed a separate kind of jurisdiction have ignored the exact nature of the jurisdiction of criminal justice, that is, the power of a state over a criminal for his or her crime. Once the power of the state is denied,

there will be no jurisdiction. The imagination of changing cyberspace into an independent sovereign space has nothing to do with criminal justice.

In sum, what criminal jurisdiction responds to the question of criminal liability borne by the criminal and based on a criminal act. It will be clearer if we take an example from the Finnish Penal Code. Chapter 17 Section 16 (563/1998) of the Code provides that organized gambling is the act of unlawfully arranging gambling or keeping a room or other premises for gambling, or where the proprietor of a hotel or restaurant establishment allows gambling to take place.[208] The establishment of jurisdiction has to satisfy two prerequisites: a space for gambling, and "games and activities" that can be categorized as gambling. In order to extend the validity of this clause to online gambling and establish jurisdiction, a web site has to be regarded as a similar place to a room or other premises, while clicking with a computer mouse in the face of a screen on which "gambling" is taking place should be regarded as the equivalent of "gambling." Finally, organizing gambling in such a place has to be prescribed explicitly in the laws or regulations so as to provide the basis for liability and thus the basis for jurisdiction.

8.7 Critical factors in cybercriminal jurisdiction

208 Here, "Gambling means pools, bingo, tote and betting games, money and goods lotteries, casino operations and other similar games and activities where winning is completely or partially dependent on chance or events beyond the control of the participants in the game or activity and where the possible loss is clearly disproportionate to at least one of the participants' ability to pay up." Penal Code of Finland, Chapter 17, Section 16 (563/1998).

After examining most of the plans for jurisdiction over cybercrimes, it is clear that no single plan can solve all the problems. Any plan has both advantages and disadvantages. Furthermore, some new plans have no practical meaning for the field of criminal justice, but only for civil and administrative cases. Although cybercrime is different from traditional crimes, it is impossible to abandon completely the traditional criminal-justice system. This chapter attempts to collect some factors for a seemingly comprehensive solution to the question of jurisdiction over cybercrime. This solution is based on the idea that jurisdiction over cybercrime can be flexibly based on traditional jurisdiction, and supplemented by jurisdiction over the location of the computer from which the most direct demand was made. The aim of the plan is to explore the possibility of solving the question of jurisdiction over most cybercrime cases.

The main issue in a jurisdiction based on the location of the act is that a cybercrime case may involve multiple places. It is significant to determine the place where the computer is from which the most direct command was sent, such as the location of the computer from which the intrusion command was made, the location of the computer from which the illegal contents and viruses were published, and the location of the computer from which the command for a distributed denial-of-services attack was made. This is in fact an alternative to the jurisdiction based on the location of the act, in which tools of the act are identifiable. Generally, this location is most closely linked to the perpetrator, and it is convenient to collect evidence and arrest the suspect. But if the victims are concentrated in a certain place, for example the attack is targeted at information systems of a web site, a server, an institution, or even a state, the more convenient way is to hold the perpetrators liable at the location where the

victims are situated.

In intrusion cases, there must be a computer used in the offence, or alternatively, there must be an IP address. Even if the perpetrator uses the dynamic IP address, or conceals the real IP address, it is not completely impossible to trace back the real location. Notwithstanding this, the process may turn out to be more complicated, and the cost may be more expensive.

In content- or security-related offences, if the owner of the web site, manager, administrator, and perpetrator is an identical figure, jurisdiction based on the computer from which the direct command was made is possible. If they are different, according to the principle of individual liability, it is necessary to find the perpetrator in the location of the computer from which the direct command was made.

In distributed denial of services attacks, if thousands of computers are manoeuvred so as to launch attacks, it is far from easy to determine the location of the relevant jurisdiction. Most of these computers may belong to innocent third parties. Therefore, the location of the computer from which the command was sent must be identified. There may be one location or more locations subsequently or simultaneously. The principle should be to establish jurisdiction through any one of the locations. If the crime is committed by multiple perpetrators in many locations, the jurisdiction should once again be coordinated.

The registration place of a web site can be an alternative to nexus of active nationality, that is, the nationality of the corporation. In cases of web sites providing obscene materials, or gambling services, jurisdiction established on this basis can avoid the loophole where the perpetrator escapes jurisdiction on

ground of his personal nationality. If an individual in State A registers a web site in State B, and as a result the residents in State C are victimized, State B should hold the individual liable. In this case, the location of the server is difficult to determine. However, when the substantial location of the web site is where it was registered, jurisdiction over this offence should be directed to the registration location.

It is possible for the perpetrator to escape the law of the state of his nationality, and register the web site in a state that does not criminalize the act. In this case, the only feasible way is to the coordinate laws between these states. If it is impossible to coordinate laws -as in most cases, and the state of registration does not prosecute the case according to its own law, the jurisdiction can also be established according to the passive nationality.

Whatever the situation, state sovereignty should be respected according to the general rule of international law. The problem should only be solved through negotiation.

In cases of the provision of illegal services, the location of the bank account used to receive payment should also be a nexus. The essence of illegal services is to make money, while the key step in making the money is to receive the payment. Therefore, the location where the payment is received is critical in establishing jurisdiction. Receiving money is a part of the criminal act, and has direct link with the perpetrator. Although there is a possibility that payment may pass through many countries, the final account must be located in one or more specific states. Jurisdiction based on these locations is significant. If it is impossible for this state to prosecute, it remains feasible to apply the jurisdiction of passive nationality.

In the case of online sales of goods, jurisdiction should be based on the nexus of location where the controlled articles are situated. In the online transaction of legal goods, there is a deposit location and a consignment location, usually involving individuals who are directly responsible for the transaction. If other liable persons are traceable, the case can be investigated or prosecuted by the authorities of the state where the act has been committed or the state of nationality. If they are not traceable, the individuals directly involved in the consignment of the goods should be investigated so as to find more clues. The goods should also be sealed and distrained. If this state cannot investigate on grounds its own law, jurisdiction according to the passive nationality or protection jurisdiction should be applied.

In cyber terrorist cases and other crimes prescribed in international law, the establishment of universal jurisdiction is inevitable. A kind of super-national jurisdiction is also possible where dual criminality is not the prerequisite as in traditional criminal law. Regionally, the Convention on Cybercrime requires member parties to establish a jurisdiction sufficient to hold most of the offenders liable for their activities which are prohibited by the Convention. A similar treaty is the UN Convention against Trans-national Organized Crime, which offers great potential for enhanced cooperation among countries with respect to the implementation of anti-money laundering measures inevitably related to the abuse of computer networks.

8.8 Conclusion

Because of the wide existence of cybercriminals and the lack of legal consensus, cyberjurisdiction is becoming a problem that legislation and law enforcement must face. The challenge is to create rules that work smoothly across local, national, and international boundaries.

In order to rebuild the basis for jurisdiction, countries have passed laws or make precedents to cover cybercrime under domestic power. As far as the expanding of the principle of territorial jurisdiction is concerned, theoretical and practical efforts have been made to create new jurisdictional links between the power of the authorities and the events. The book evaluates the theory of web site locus jurisdiction and the theory of the limited expansion of the principle of territorial jurisdiction. On the other hand, significant efforts have also been made to establish new jurisdictional principles, including theory of the new sovereignty, and the theory of international space.

However, all these efforts are limited in the scope of their application. A comprehensive consideration of factors needed for solving the issue of jurisdiction over cybercrime is discussed in this chapter, with the purpose for establishing the grounds for a jurisdiction based mainly on traditional criminal-law theory and according to different situations in cybercrime cases. Practically speaking, traditional legal framework may have the potential to extend its domain to cyberspace with respect to jurisdiction. For example, the Penal Code of Finland prescribes that where "there is no certainty of the place of commission, but there is a justified reason to believe that the offence was committed in the territory of Finland, it is deemed to have been committed in Finland."[209]

[209] Penal Code of Finland (39/1889), Chapter 1, Section 10 (4).

In shifting the emphasis of jurisdiction over cyberspace from a territoriality-dependent crime scene to a territoriality independent crime scene, a comprehensive scheme should be drawn up to reach full coverage of the complicated situations. Successful trans-border prosecutions have proved that law enforcement is not without resources when there is an urgent call for international assistance, regardless of state boundaries. One of the more striking examples is the Operation Predator operation. Since 9 July 2003, the U. S. Immigration and Customs Enforcement (ICE) have launched the Operation Predator programme to investigate paedophiles, human traffickers, international sex tourists, and individuals who trade in child pornography. The achievements of the ICE have been approximately 7,000 arrests of individuals in the U. S. and 13 other countries as a result of information provided by the ICE itself.[210]

Jurisdiction is not the only factor, but it is the most important one necessitating international cooperation. However, one of the prior premises for the resolution of the jurisdictional problem is the harmonization of substantive law. The next chapter will give a brief sketch of the international efforts to harmonize cybercrime law.

210 U. S. Immigration and Customs Enforcement, Austrian Authorities Act on ICE Leads; Execute 120 Search Warrants in Massive Child Pornography Probe, 13 June 2005. Retrieved 15 February 2016, from http://usinfo.state.gov/gi/Archive/2005/Jun/14-475154.html

CHAPTER 9 INTERNATIONAL ACTIONS AGAINST CRIMINALITY[211]

9.1 Introduction

Traditionally, crime and punishment are largely local, regional, or national. Today, many differences confronting us are associated with the transnational character of cybercrimes. It is therefore important to have international legal instruments ready to serve anti-crime efforts.

This chapter looks at international harmonizing efforts to fortify the legal battle against cybercrime, categorizing the actions into four aspects: professional law-enforcement efforts, regional efforts, multi-national efforts, and global international efforts. Subsequently, the chapter also categorizes the international actions according to the subject-matters into additional aspects, including the promotion of security awareness at both international and national levels, the harmonization of legislation, coordination and cooperation between law-enforcement agencies, and direct anti-cybercrime actions. The chapter will also examine the nations' attitudes toward the Convention on Cybercrime. Based on

[211] This chapter is based on Li 2007a, with updated information.

the analysis, the chapter will briefly evaluate the effectiveness of previous attempt at international harmonization.

9.2 From domestic legislation to international harmonization

People usually are impressed by the illusory overlap between Internet space and international space. Notwithstanding the fact that information systems are linking continents, islands, residents and communities into a giant virtual network, states and areas preserve their traditional sovereignty. McConnell International's metaphor (2000, p. 8) said that: "In the networked world, no island is an island." At this turning point, the globally connected Internet has made cybercrime a trans-border problem. The "international dimension" (Wasik 1991, pp. 187-201), "trans-national dimension" (Sofaer and Goodman 2005) or "global dimension" (Grabosky 2004, pp. 146-157) of cybercrime is universally perceived. The following figure shows how cybercrime is distributed in 20 countries of the world:

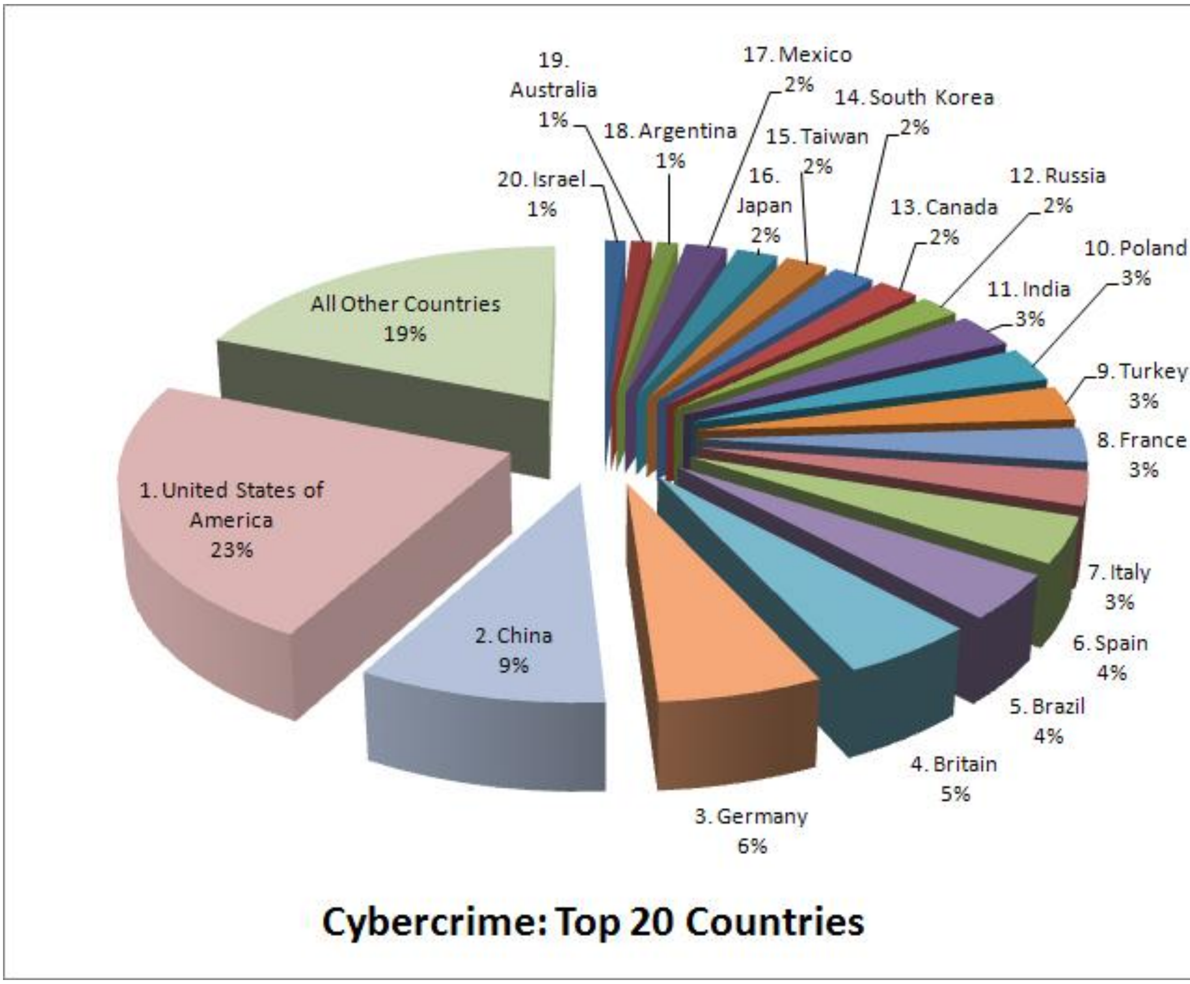


Figure 5 List of Top 20 Countries with the Highest Rate of Cybercrime

(Credit: BusinessWeek/Symantec 2012. Retrieved 15 February 2016, from http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/)

While law is always territory-based, the tool, the scene, the target, and the subject of cybercrime are all boundary-independent. Domestic measures will certainly be of critical importance but not sufficient for meeting this worldwide challenge. International coordination and cooperation are necessary in fighting offences commonly prohibited by every country.

Many international organizations have been making efforts to harmonize actions within their forums. Many authors have also been pursuing research on international harmonization from different standpoints and for different goals; for example, Sieber (1996, 1998), United Nations Crime and Justice Information Network (UNCJIN) (1999), Police Commissioners' Conference Electronic Crime Working Party (2000), Sofaer and co-workers (2000), Putman and Elliott (2001), Schjolberg (2005), and so on. Although information about the basic facts of international harmonization that these research studies deal with is the same, different knowledge can be drawn from different thinking. For the purpose of convenient summarization within this chapter, I categorize the international harmonization actions into the following groups: professional organizations, regional organizations, multi-national organizations, and global organizations (See Table 3). Many other valuable international actions have simply not been considered due to the limit of this study (it is hardly possible to assume that studies on cybercrime can cover all useful international actions of international organizations at all levels).

Table 4 Categories of International Harmonization Concerning Cybercrime

Categories	Subjects	Member States (as of March 2007)	Major Actions (including but not limited to)
Professional organization	Interpol	190	Legal harmonization; Coordination and

			cooperation in law enforcement; Direct actions
Regional organizations	APEC	21	Promotion of security awareness on international level; Promotion of security awareness on state level; Legal harmonization
	African Union	54	Promotion of security awareness on international level; Promotion of security awareness on state level; Legal harmonization
	Council of Europe	47	Coordination and cooperation in law enforcement; Legal harmonization
	EU	28	Coordination and cooperation in law enforcement; Legal harmonization
	OAS	35	Coordination and cooperation in law enforcement; Legal harmonization

Multinational organizations	Commonwealth of Nations	53	Legal harmonization
	Group of Eight	8	Promotion of security awareness on international level; Coordination and cooperation in law enforcement; Legal harmonization.
	OECD	34	Direct actions against cybercrime
Global organization	United Nations	193	Promotion of security awareness on international level

9.3 Professional efforts of the International Criminal Police Organization (Interpol)

Many international organizations qualify for professional organizations, because their goals and activities are focused on certain specific issues; these organizations include Interpol, the International Telecommunications Union, etc. However, professional efforts here primarily mean substantial actions in the field of cybersecurity protection and cybercrime prevention. Although some other organizations also greatly contribute to coordinating cybersecurity protection, their emphasis is not necessarily on the law. By this standard, this

section only analyses the actions of the International Criminal Police Organization (Interpol).[212]

As an international law-enforcement organization with 190 members, Interpol started to tackle computer crime very early, coordinating law-enforcement agencies and legislations, in regard to which Interpol made efforts to improve counter-cybercrime capacity at the international level. A 1981 survey of members on cybercriminal law recognized dilemmas in application of existing legislation (Schjolberg 2004). Based on the recognition of the legal gaps between countries, and gaps between the legal framework and criminal phenomena, Interpol expanded its task to both law enforcement and legal harmonization.

Currently, there are four working parties within the framework of Interpol, comprising African, American, Asia-South Pacific and European Working Parties on Information Technology Crime. Besides these groups, a Steering Committee for Information Technology Crime was established in order to harmonize the different regional working-party initiatives.[213] Considering the already-harmonized legislation as the prerequisite for the coordinated law enforcement, the African Working Party agreed upon "the project on legislation and comparative law existing in the Africa with a view to having more African states co-signing and/or ratifying the Council of Europe Cybercrime

---

212 For a general analysis of Interpol as "a world crime-fighting organization that has puzzled three generations of scholars, law-enforcement officers, and legislations," see Fooner (1989).

213 See Interpol web site for detailed introduction to the functions and activities of these working parties and the steering committee, at http://www.interpol.net/Public/TechnologyCrime/WorkingParties/Default.asp

Convention."[214] Apparently, legal harmonization is one of Interpol's important tasks in working towards an effective law-enforcement environment.

In 2010, the Interpol Global Complex for Innovation (IGCI) was established in Singapore as a cutting-edge research and development facility for the identification of crimes and criminals, innovative training, operational support and partnerships. The Global Complex goes beyond the traditional reactive law enforcement model. This new centre provides proactive research into new areas and latest training techniques. The aim is to give police around the world both the tools and capabilities to confront the increasingly ingenious and sophisticated challenges posed by criminals.

In regard to law enforcement, Interpol has provided a technical guidance in cybercrime detection, investigation and evidence collection. The Interpol Information Technology Crime Investigation Manual was compiled by the European Working Party on Information Technology Crime.[215] Compared with the substantive and procedural law harmonization of today's Convention on Cybercrime, the Manual developed a technological law-enforcement model to improve the efficiency of combating cybercrime.

Along with efforts in law enforcement on cybercrime, Interpol also takes distinct actions to prevent cybercrime, cooperating with credit-card companies to combat payment fraud by building a database on Interpol's web site (Police Commissioners' Conference Electronic Crime Working Party 2000, p. 64). As one of the necessary cooperation projects at the international level of law-enforcement, cybercrime and other trans-border crimes are specially dealt with

---

[214] ibid.
[215] ibid.

by Interpol in gathering and sharing information. In addition, Interpol is making efforts to establish a network to for harvesting information relating to activities on the Internet.[216]

International facilitation through Interpol's global network connected investigators across the globe and resulted in the arrest of more than two dozen people involved in two related cases of payment card fraud where a total of USD 45 million was stolen worldwide. Known as an 'ATM cash-out scheme', this sophisticated crime occurs when a cybercrime organization hacks into the networks of payment card companies to steal the card numbers, as well as remove any spending or withdrawal limits. The card numbers are then sent out to members of the network around the world, who code them onto blank cards and use them to withdraw massive amounts of cash from bank machines. In December 2012, hackers stole the card numbers of prepaid debit cards issued by a bank in the Middle East. The card numbers were used to with withdraw some USD 5 million in cash from bank machines across 20 countries. Soon after, the same cybercriminal network hacked into another payment card processing system and accessed the numbers for cards issued by a second Middle Eastern bank. In this case, the criminals made off with USD 40 million from bank machines in 25 countries. Between the two cases, the criminals stole money via bank machines in a total of 26 countries worldwide, including Canada, Colombia, Japan, Egypt, Romania, Russia, Sri Lanka, the UK and the US. The money was laundered through purchases of luxury goods such as expensive watches and sports cars. Interpol played an operational support role to connect the countries investigating these cases within their respective

[216] Interpol, Interpol press release, CPN02/00/COMandPR, 5 February 2001.

jurisdictions. A working meeting organized by Interpol in early 2014 brought together investigators to discuss the details of the two thefts and to share information about the perpetrators and their known locations, and the Organization facilitated communication among investigators globally. Once the suspects were identified and located, Interpol issued Red Notices alerting police worldwide that they were wanted in connection with these crimes. To early 2014, some 25 individuals have been arrested in more than five countries (Interpol 2014a).

In a two-day (26 and 27 November) operation coordinated by Europol with the support of Interpol and Ameripol, law enforcement agencies from all over the globe, in cooperation with the airline, travel and credit card industries, undertook an action to combat online fraud. More than 60 airlines and 45 countries were involved in the activity, which took place at some 80 airports across the world. The coordinated operation targeted criminals suspected of fraudulently purchasing plane tickets online using stolen or fake credit card data. More than 281 suspicious transactions were reported during the operation, with 118 individuals arrested. Representatives from the airlines and major credit card companies American Express, MasterCard, Visa Inc. and Visa Europe were present at Europol to identify suspicious airline ticket transactions. Interpol assisted the action with the rapid identification of wanted persons and stolen travel documents detected during the operation, through the support of officers at the Interpol General Secretariat in Lyon, France, the IGCI in Singapore and at Europol. The International Air Transport Association (IATA) also took part in the action, providing important fraud intelligence from its database. Notifications were sent to transport hubs across the world as waiting law

enforcement officers intercepted and detained suspects attempting to travel using fraudulently obtained flight tickets. The banking, airline and travel sectors have suffered huge financial losses as a direct result of such Internet-facilitated crime, with the airline industry alone facing losses of USD 1 billion caused by fraudulent online ticket booking according to IATA. In addition, millions of innocent citizens are affected through the misuse of their credit card data. Besides the successful operational outcome, another positive result was the creation of a global alliance of airlines and law enforcement agencies who will be working together on an ongoing basis to combat online fraud and crime (Interpol 2014b).

In summer 2015, an Interpol-coordinated operation targeting illegal online gambling and financial fraud in Asia led to the arrest of some 48 individuals and the seizure of computers and other electronic evidence. As part of Operation Aces, which involved Cambodia, Korea, Philippines, Thailand and Vietnam, police in Thailand arrested 28 individuals of Chinese, Korean and Thai nationality accused of operating multiple illegal gambling offices handling more than USD 10 million. Six additional individuals were arrested in Cambodia. Thai police also discovered two call centre-type operations running scams targeting victims in Korea. The suspects would trick the victims into disclosing their bank account information then withdraw money from the accounts, stealing an estimated USD 200,000. Some 14 people were arrested in connection with these operations. The operation, which ran from 15 June to 31 July was coordinated by the Interpol Liaison Office in Bangkok supported by Interpol's Anti-Corruption and Financial Crimes unit and the Interpol National Central Bureau (NCB) in Bangkok (Interpol 2015a).

In November 2015, a two-day (3 and 4 November) operation was organized globally by Europol through its European Cybercrime Centre (EC3) in The Hague, the Netherlands, with support from INTERPOL through its General Secretariat headquarters in Lyon, France, Ameripol in Bogota and Canadian law enforcement authorities. The coordinated action targeted criminals suspected of fraudulently purchasing plane tickets online using stolen or fake payment card data. Law enforcement joined forces with the airline, travel and payment card industries to tackle this growing type of online fraud. The operation has led to the detention and investigation of 133 individuals suspected of using stolen payment card details to purchase airline tickets (Interpol 2015b).

Interpol launched Operation First Light 2014, which involved six countries, resulted in the arrest in Thailand of more than 20 individuals and the identification of several syndicate heads who had been generating tens of millions of dollars in illicit profits. Chinese police indicated a reduction of 40 per cent in telecom fraud as a result of the operation (Interpol 2015c).

In 2015, Interpol launched the Operation First Light 2015, resulting in more than 500 arrests and 15 call centres shut down in the Interpol-coordinated operation targeting multi-million dollar phone and email scams across the Asia Pacific region. The Operation involved 23 countries, comprised of a series of raids across the region with the largest in Indonesia where police arrested 245 Chinese and Taiwanese individuals, and in Cambodia where 168 Chinese nationals were taken into custody. Korean, Nigerian, Filipino, Russian and Taiwanese nationals were also among those arrested in China, Hong Kong (China), Korea, Thailand and Vietnam during the two-month long operation

during which more than 30 suspicious call centres were identified (Interpol 2015c).

9.4 Regional efforts

There are many regional international organizations, with a narrow or broad coverage of states, more or less making efforts to maintain cybersecurity and harmonize international measures to combat cybercrime. This section will introduce only five of these organizations, which have taken typical actions in combating cybercrime.

(1) The African Union

It was estimated by the International Telecommunications Union (ITU) that, the number of mobile subscribers reached 63 per cent in 2013 in African states, and more than 16 percent of the African population had access to the Internet (United Nations Economic Commission for Africa 2014, p.1). Similar to the developed countries, African countries is also confronted with the same threat from cybercrime. Experts estimate that 80 per cent of personal computers on the African continent are infected with viruses and other malicious software (ibid. p. 2). Cybercriminals have seen Africa as opportune to commit their criminal acts because Africa is very prone to cyber-related threats due to the high number of domains coupled with very weak network and information security (ibid. p.2).

In November 2009, the Oliver Tambo Declaration was adopted at the Extraordinary Session of the African Union (AU) Ministers in charge of ICT in

Johannesburg. This declaration asked that the AU Commission "jointly develop with the United Nations Economic Commission for Africa, under the framework of the African Information Society Initiative (AISI) a convention on cyber legislation based on the Continent's needs and which adheres to the legal and regulatory requirements on electronic transactions, cyber security, and personal data protection. It is recommended that AU Member States adopt this convention by 2012."

After consultations and regional workshops that engaged African stakeholders and international experts, the AU Commission released a draft convention that was endorsed by the AU Conference of Ministers in charge of ICT in Khartoum in September 2012. The AU adopted the Convention on Cyber Security and Personal Data Protection on 27 June 2014, at the 23rd Ordinary Session of the Summit of the AU in Malabo, Equatorial Guinea.

The Convention was intended to define the objectives and broad orientations for the information society in Africa, as well as to strengthen existing legislations in Member States and the Regional Economic Communities (RECs) on the ICTs. It defines the security rules essential to establishing a credible digital space in response to the major security related obstacles to the development of digital transactions in Africa. It lays the foundation for an African Union-wide cyber ethics and enunciates fundamental principles in the key areas of cyber security. It also defines the basis for electronic commerce, puts in place a mechanism for combating intrusions into private life likely to be generated by the gathering, processing, transmission, storage and use of

personal data and sets broad guidelines for incrimination and repression of cyber crime.[217]

The convention attempts to address a wide range of online activities, including electronic commerce, data protection, cybersecurity and cybercrime. Regarding cybercrime, it requires African states to adopt laws that criminalise:

1. Attacks on computer systems (e.g. fraudulently accessing a computer system);

2. Computerised data breaches (e.g. fraudulently intercepting data);

3. Content-related offences (e.g. disseminating child pornography);

4. Offences relating to electronic message security measures.

In addition, the convention emphasises the importance of enhancing international cooperation to fight cybercrime. Article 28 requires states to harmonise cybercrime legislation and regulations to "respect the principle of double criminal liability."

In order to facilitate information-sharing across borders and enhance collaboration on a bilateral and multilateral basis, the convention calls on states without cybercrime mutual legal assistance agreements to try to rectify this deficit.

The convention recognises that building capacity to fight cybercrime is essential, requiring African states to establish appropriate institutions to combat cybercrime and to offer training to those stakeholders tasked with fighting cybercrime.

Furthermore, the Convention requires that African states enact cybercrime offences that "are punishable by effective, proportionate and dissuasive criminal

---

217 Retrieved 15 February 2016, from http://au.int/en/cyberlegislation.

penalties". The convention thus rightly emphasises the need to create sufficient deterrents to reverse the status quo of criminals turning to cybercrime because it is low risk.

Article 32 designates the AU Commission Chairperson as responsible for overseeing the establishment and monitoring of the convention. Among other responsibilities, the Chairperson is required to:

1. Encourage African states to adopt and implement the convention's measures

2. Advise African states on how to promote cybersecurity and combat the scourge of cybercrime at a national level

3. Analyse the nature and magnitude of cybercrime, including gathering information about cybercrime activity in Africa and transmitting such information to the competent national authorities

4. Establish partnerships with African civil society and governmental, intergovernmental and non-governmental organisations in order to facilitate dialogue on combating cybercrime

5. Submit regular reports on the progress made by each African state in the implementation of the convention's provisions.

Fifteen countries must ratify the convention before it enters into force. Unfortunately, no countries have done so and the AU faces substantial challenges in convincing states to support the convention and implement its provisions. There are serious concerns about its human rights implications, particularly about provisions that might support discrimination and expand government power, even though several have enacted or proposed domestic cybersecurity legislation (Fidler 2015).

(2) The Asia-Pacific Economic Cooperation (APEC)

In the Asia-Pacific region, APEC coordinates its 21 member economies to promote cybersecurity and to tackle the risks brought about by cybercrime (APEC 2003). APEC has conducted a capacity-building project on cybercrime for member economies in relation to legal structures and investigative abilities, where the advanced APEC economies support other member-economies in training legislative and investigative personnel.[218]

After the 9/11 attacks on the U. S., the APEC Leaders issued a Statement on Counter-Terrorism, condemning terrorist attacks and considering it urgent to reinforce collaboration at different layers to fight against terrorism. The Leaders called for reinforcing APEC activities to protect critical infrastructure.[219]

The Telecommunications and Information Ministers of the APEC economies issued the Statement on the Security of Information and Communications Infrastructures and a Programme of Action in 2002,[220] supporting measures taken by members to fight against misuse of information. The Senior Officials' Meeting has made a recommendation which designates six areas that can serve as the foundation for APEC's endeavour for cybercrime prevention, comprising legal development, information sharing and cooperation, security and technical guidelines, public awareness, training and

---

218 Cybercrime Expert Group, Proposal, Doc no: telwg29/ESTC/12, APEC Telecommunications and Information Working Group, 29th Meeting, 21-26 March 2004, Hong Kong, China.

219 APEC Leaders Statement on Counter-terrorism, APEC Economic Leaders' Meeting, Shanghai, 21 October 2001.

220 APEC, Recommendation by the APEC Telecommunications and Information Working Group (TEL) to APEC Senior Officials (SOM) for an APEC Cybersecurity Strategy, 2002/CSOM/052, Concluding Senior Officials Meeting, Los Cabos, B.C.S., Mexico, 21-22 October, 2002.

education, and wireless security.[221] The Ministers and Leaders of APEC have made a commitment to "endeavour to enact a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with the provisions of international legal instruments, including the UN General Assembly Resolution 55/63 and Convention on Cybercrime by October 2003."[222]

In response to this call from the leaders, a survey of laws was carried out and a summary was made of the responses from member economies received in 2003 (See E-Security Task Group 2003). The economies proposed corresponding projects in information-security task groups. For example, the U. S. proposed a project in the e-Security Task Group of the Telecommunications and Information Working Group. The first phase of this project was a meeting of cybercrime experts from around the region. The meeting was held from 21-25 July, 2003 in Bangkok, Thailand, and was attended by over 120 delegates from 17 economies. The objectives of the meeting were to assist the economies to develop the necessary legal frameworks; to promote the development of law-enforcement capacity; and to strengthen cooperation between private and public sectors in addressing the threat of cybercrime.[223] In the conference, the experts present agreed that every economy needed a legal framework including one for substantive and procedural law, and for the law and policies of inter-economies cooperation. They confirmed the role of international instruments, particularly the Convention on Cybercrime. They also emphasized jurisdictional

221 ibid.

222 Cybercrime Expert Group, Proposal, Doc no: telwg29/ESTC/12, APEC Telecommunications and Information Working Group, 29th Meeting, Hong Kong, China, 21-26 March 2004.

223 See APEC, Cyber Security Workshop Summary, 2003/SOMIII/ECSG/021, Electronic Commerce Steering Group Meeting Phuket, Thailand 15-16 August 2003.

cooperation, law-enforcement construction, and the capacity building of the investigators.[224]

In 2005, The sixth APEC Ministerial Meeting on the Telecommunications and Information Industry passed the Lima Declaration, "encouraging all economies to study the Convention on Cybercrime (2001) and to endeavour to enact a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with international legal instruments, including UN General Assembly Resolution 55/63 (2000) and the Convention on Cybercrime (2001)."[225] However, due to the great difference between member economies within APEC, the development toward unified legal instruments has not been too satisfactory. Although some economies have claimed that their laws have been completely consistent with the Convention, and some other economies were taking actions to implement provisions similar to the Convention, many other countries have quite different legal systems or have no law criminalizing cybercrime.

Efforts are still to be made in the forum of APEC to address cybercrime. The U.S. proposed the Judge and Prosecutor Cybercrime Capacity Building Project in 2006 in order to develop a curriculum devised by government and private sector experts; to translate the curriculum into domestic languages; and to train the trainer (judges and prosecutors).[226]

224 APEC, Conference on the Strengthening International Law-enforcement Cooperation to Prosecute Cyber Criminals, Hackers, and Virus Authors, Media Release, Bangkok, 25 July 2003.

225 Article 26 of Lima declaration, The 6th APEC Ministerial Meeting on the Telecommunications and Information Industry (TELMING, 1-3 June, 2005, Lima, Peru).

226 APEC, 2006 Budget – Operational Account Project: TEL 04/2006 – Judge and Prosecutor Cybercrime Capacity Building Project, 2006/BMC1/012-6, Budget and

In 2010, the 8th Ministerial Meeting on Telecommunications and Information endorsed the Strategic Plan for 2010-2015, including promotion of a safe and trusted ICT environment. They plan emphasizes the need for enhanced measures to address malicious online activities (Section 19), and encourages each economy to enhance mutual cooperation on countering malicious online activities, to engage in efforts to increase cybersecurity awareness and to share information on protecting ICT. These efforts need to align with efforts by and in collaboration with industry partners, the Internet technical community and all other relevant stakeholders including Internet Service Providers (ISPs), telecom operators as well as regional and other international organizations. Such efforts will foster a more secure online environment that protects ICT networks and users and secures access to information in an appropriate manner (Section 20).

In 2011, the 44th Meeting of the Telecommunications and Information Working Group was held in Kuala Lumpur, Malaysia. A Cybercrime Experts Group Meeting was held in conjunction with this Working Group meeting, and a mission statement was adopted as follows: "The Security and Prosperity Steering Group (SPSG) Experts Group on Cybercrime will further the APEC leaders statements and the goals of the SPSG to promote cybersecurity by strengthening the capacity of members economies to detect, investigate and prosecute cybercrime, and to promote and improve cooperation among member economies in the fight against cyber crime."

In 2015, the 10th Ministerial Meeting on Telecommunications and Information (TELMIN10) endorsed the Strategic Plan for 2016-2020, with

---

Management Committee Meeting I, APEC Secretariat, Singapore, 29-30 March 2006

priority areas to develop and support information and communications technologies ICT innovation; promote a secure, resilient and trusted ICT environment; promote regional economic integration; enhance the Digital Economy and the Internet Economy; and strengthen cooperation.

(3) The Council of Europe (CoE)

The Council of Europe has been working to tackle rising international anxiety over the risks brought about by the automatic processing of personal data since the early 1980s.[227] In 1981, the Council of Europe implemented the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data,[228] which was revised according to the Amendment to Convention ETS No. 108 Allowing the European Community to Accede, 15 June 1999, and the Additional Protocol to Convention ETS No. 108 on Supervisory Authorities and Trans-border Data Flows, 8 June 2000. The Convention recognized the desirability "to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing," and the necessity "to reconcile the fundamental values of the respect to privacy and the free flow of information between peoples" (Preamble). The Convention covers the protection of personal data in both the public and private sectors.

Chapter II of the Convention established basic principles for data protection, one of which is data security (Article 7), covering the prohibition of

---

[227] For example, on 13 September 1989, the Committee of Ministers of the Council of Europe adopted Recommendation R (89) 9 of the Council of Europe on Computer-Related Crime, which contained guidelines for national legislatures.

[228] ETS No. 108, 26 January 1981.

accidental or unauthorized access, alteration and dissemination.

The expert committee appointed in 1985 published Recommendations of 1989 and 1995, addressing the issues of substantive laws and procedural law in this area respectively.[229]

Recommendation R. No. (89) 9 recognized the importance of an adequate and quick response to the new challenge of computer-related crime, which often has a trans-border character, and recommended the governments to consider the Report on Computer-Related Crime drawn up by the European Committee on Crime Problems.

Then there is Recommendation No. (95) 13 Concerning Problems of Criminal Procedure Law Connected with Information Technology. The Recommendation recognized that information systems may also be used for committing criminal offences, evidence of criminal offences may be stored and transferred by these systems, while the criminal procedure law of member states often do not provide for appropriate powers to search and collect evidence in these systems during a criminal investigation. The appendix to the Recommendation lays down the principles for criminal procedure laws on search and seize, technical surveillance, obligations to co-operate with the investigating authorities, electronic evidence, use of encryption in research, statistics and training, and international cooperation.

In 1997, the Council of Europe began drafting the Convention on Cybercrime, which was open for signature in 2001 and took effect in 2004.[230] In 2003, the Additional Protocol to the Convention on Cybercrime Concerning

---

229 See Recommendation No. R. (95) 13.

230 See Council of Europe, Convention on Cybercrime, CETS No.185, status as of 20 March, 2006.

the Criminalization of Acts of a Racist and Xenophobic Nature Committed Through Computer System (ETS NO. 189) was implemented. The Convention addresses substantive law, procedural law, jurisdiction, and international law in the field of cybercrime. The Convention is a historic landmark in the combat against cybercrime.[231] It is expected that the Convention will have a deep impact on the legal reform relating to cybercrime in its 46 member states and one candidate state.

In the 2004 Conference on Cybercrime, the Council of Europe called for "wide and rapid" access to and "effective implementation" of the Convention on Cybercrime, raising awareness in the highest political level, and encouraging cooperation between public and private sectors.[232]

On the 2005 Conference on Cybercrime, the Council of Europe expressed concern about the fast-increasing threats and serious social and economic results of cybercrime including terrorist activity on the Internet, noting that most cybercrime is international cybercrime, recognized the need for effective and compatible laws and tools to enable efficient cooperation to combat cybercrime, calling upon public and private cooperation, and encouraging access to the Convention on Cybercrime.[233]

In 2006, the Council of Europe launched a Project against Cybercrime, intended to grant assistance to the development of national legislation in line with the provision of the Convention, training of judges, prosecutors and law-enforcement officers, and training of criminal justice officials and 24/5 contact

---

231 For more detailed discussion. See infra Section 6.

232 Council of Europe, Conference on The Challenge of Cybercrime, 15-17 September 2004, Palais de l'Europe, Strasbourg, France.

233 Council of Europe, Cybercrime: A Global Challenge, A Global Response, Casa de America, Madrid, Spain, 12-13 December 2005, CYB (2005) Conclusions.

points in international cooperation.

(4) The European Union

The EU took a series of actions to tackle cybercrime through impelling a coordinated law enforcement and legal harmonization policy. Civil liberty has also been a focus in the anti-cybercrime field.

In 1995, the European Parliament and the Council endorsed Directive 95/46/EC of 24 October 1995 on the protection of Individuals with regard to the Processing of Personal Data and on the Movement of Such Data. Section VIII of the Directive specifically deals with confidentiality and security of processing of personal data. The Directive applied to protection of natural persons (Article 2(a)). The scope of the Directive was limited to the processing of personal data entirely or partially by automatic means (Article 3-1). The Directive required that appropriate technical and organizational measures have to be implemented to protect personal data against illegal destruction, alteration, access and other illegal forms of processing (Article 17-1).

The Directive required the Member States to provide administrative and judicial remedies for the victim (Article 22), and provided for the compensation liability of (Article 23) and sanctions on (Article 24) the transgressor.

In 1997, the European Parliament and the Council endorsed Directive 97/66/EC of 15 December 1997 concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector. The Directive was aimed at furthering the protection implemented in Directive 95/46/EC, and providing for the harmonization of the Member States' provision to attain an equivalent level of protection (Article 1-1). The Directive extended the protection of legitimate interests to legal persons (Article 1-2).

The application scope of the Directive was limited to the processing of personal data relating to the provision of publicly available telecommunications services in the public telecommunications networks; particularly via the ISDN (Integrated Services Digital Network), and public digital mobile networks (Article 3-1). As the Directive 95/46/EC is concerned with automatic processing systems, Directive 97/66/EC has emphasized the linkage with the telecommunications network. The Directive provides requirements directly targeted at the service providers (but not member states) "to take appropriate technical and organizational measures to safeguard the security of its services." (Article 4-1). The Directive requires the Member States to implement the regulations ensuring the confidentiality of communications, prohibiting listening, tapping, storage or other kinds of interception or surveillance of communications by unauthorized natural and legal persons (Article 5). The Directive limited unsolicited communications (Article 12), which covers automatic calling systems or facsimile machines, but not e-mails.

On 27 November 2001, a plenary session took place in Brussels of the EU Forum on Cybercrime, organized by the EC,[234] and where the primary discussion was about the retention of traffic data (EU Forum on Cybercrime 2001).

In April 2002, the Commission of the European Communities presented a Proposal for a Council Framework Decision on Attacks against information systems, and this proposal constitutes the case of the Decision of 24 February

[234] European Commission, EU Forum on Cybercrime, Plenary session, Brussels, November 27, 2001.

2005.[235] The Framework Decision criminalized the offences of illegal access to information systems (Article 2), illegal system interference (Article 3), illegal data interference (Article 4), and instigation, aiding and abetting of these offences or attempt at them (Article 5). The Framework Decision only dealt with attacks through unauthorized access to or interference with information systems or data. According to the Decision, illegal access can only be constituted when the illegal activities are targeted intentionally against an "information system with specific protection measures in place and [the attacks] must be for economic gain." (Article 2)

The Commission further considered the future possibility of "specific protection measures" (Proposal for a Council Framework Decision on Attacks against information systems) to broadband networks, saying that, "it is necessary that criminal law covers unauthorized access to their systems even though there may not be adequate technical protection for their systems." (ibid.) Thus, concerning the interference with information systems, it is constituted by serious "hindering" or "interrupting" of the functioning of information systems by "inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data" (Article 3).

This Framework Decision does not specify penalties for illegal access to information systems and instigation, aiding and abetting and attempting of these offences, but requires member states to take the necessary measures to ensure that they are punishable by effective, proportional and dissuasive criminal penalties (Framework Decision, Article 6.1). The Decision specifies the

[235] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, Official Journal L 069, 16/03/2005 P. 0067 – 0071.

penalties for illegal system interference and illegal data interference as punishable by criminal penalties to a maximum of at least one to three years of imprisonment (Article 6.2). As for the "aggravating circumstances", the criminal draws a maximum of at least two to five years imprisonment (Article 7.1). These aggravating circumstances include an organized attack, and an attack that has "caused serious damages or has affected essential interests" (Article 7.2). Criminal organization is defined as a "structured association, established over a period of time, of two or more persons, acting in a concerted manner with a view to committing offences."[236]

It is worth noting that the matters mentioned in the Framework Decision can also be found in the Convention on Cybercrime.[237] After revision of the legislation required by the Convention, the national law (of Finland) will also meet the demand of the Framework Decision.[238] Today, comprised of 27 member states and three candidate countries, the EU remains active in addressing cybercrime.

(5) The Organization of American States (OAS)

As other regional organizations, the Organization of American States (OAS) with 35 member states is also highly concerned about the issue of cybercrime. Through its forum for the Ministers of Justice or of the Ministers or Attorneys General of the Americas (REMJA), the OAS has long recognized the central role that a sound legal framework plays in combating cybercrime and protecting the Internet. Such recognition has prompted the REMJA to

---

236 Article 1, Joint Action 98/733/JHA of 21 December, 1998 adopted by the Council on the Basis of Article K.3 of the Treaty on European Union, Official Journal L 351, 29 December, 1998.

237 HE 153/2006, Detailed Justifications, 2. Framework Decision and Valid Legislation.

238 ibid.

recommend the creation of the Group of Governmental Experts on Cybercrime (The Group of Experts) in March 1999.[239] The Group of Experts has been devoted to analysing cybercrimes, to inspecting the domestic cybercrime law, and to finding ways of cooperating in the Inter-American system of combating cybercrime. The Group of Experts has held four meetings.[240]

The Meeting of the Ministers of Justice or of the Ministers or Attorneys General of the Americas (REMJA III)[241] has urged member states to take steps to endorse cybercrime law; harmonize cybercrime laws to make international cooperation possible. The Meeting of the Ministers of Justice or of the Ministers or Attorneys General of the Americas (REMJA V) [242] has recommended that member states evaluate the advisability of implementing the principles of the Convention on Cybercrime, and consider the possibility of acceding to that Convention.

In 2004, the Fourth Plenary Session of the Organization of American States General Assembly passed the resolution on "Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity, " proposing that "An effective cybersecurity strategy must

---

[239] Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA II), Chapter V.

[240] The First Meeting and Second Meeting were held in May and October 1999, separately, the Third Meeting in June 2003, the Fourth Meeting in February 2006, all in Washington D. C. U. S. See OAS web site, at http://www.oas.org/juridico/english/cyber_experts.htm

[241] Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA III), Chapter IV.

[242] Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA V), Appendix I.

recognize that the security of the network of information systems that comprise the Internet requires a partnership between government and industry."[243]

9.5 Multi-national efforts

Unlike professional organizations that are limited to a more specific field of concern, and unlike regional organizations that are limited to a more specific location of states, the multi-national international organizations care for affairs of a broader range and take actions in a broader territorial environment. This section recounts the efforts of three of the multi-national organizations.

(1) The Commonwealth of Nations

The Commonwealth of Nations took a direct and timely action in the harmonizing laws of its member states. In October 2002, the Commonwealth Secretariat prepared the "Model Law on Computer and Computer Related Crime" (Bourne 2002, p. 17). Within the Commonwealth's 53 member countries, the "Model Law" has had a wide influence on domestic legislation. Through this model law, the Convention on Cybercrime has become one of the legislative choices in substantive criminal law, covering the offences of illegal access, interfering with data, interfering with computer systems, illegal interception of data, illegal data, and child pornography.

Compared with the Convention on Cybercrime, the Model Law expanded

243 AG/RES. 2040 (XXXIV-O/04), Adopted at the fourth plenary session of the Organization of American States General Assembly held on 8 June 2004 in Quito, Ecuador.

criminal liability –so as to include reckless liability- for the offences of interfering with data, interfering with computer systems, and using illegal devices. The Model Law also covered the problem of dual criminality by stating that the act applied to an act done or an omission made by a national of a state outside its territory, if the person's conduct would also constitute an offence under a law of the country where the offence was committed. This may lead to prosecution or extradition based on dual criminality, but not extradition as it is provided in the Convention on Cybercrime.[244]

Some of the member countries of the Commonwealth have made efforts to draft domestic law according to the model law, such as Bahamas and St. Lucia.[245] In Barbados, Belize, and Guyana, the Model Law is being considered as a guide to the enactment of similar legislation.[246] However, in many other countries of the Commonwealth, there is still no special legislation for cybercrime.[247]

Besides impelling legislation within the forum, another focus of the Commonwealth is on mutual assistance in law enforcement between Commonwealth member states and between Commonwealth member states and non-Commonwealth states. In the 2005 Meeting of Commonwealth Law Ministers and Senior Officials, the Expert Working Group proposed 10 recommendations for member states to adopt suitable measures for improving domestic law enforcement and trans-national assistance, and encouraged

---

244 Legal and Constitutional Affairs Division Commonwealth Secretariat, Report on Law and Technology Workshop for the Caribbean, Kingston, Jamaica, 3-7 November, 2003, published in January, 2004.

245 ibid.

246 ibid.

247 ibid.

member states to sign, ratify, accede to and implement the Convention on Cybercrime as a basis for mutual legal assistance between Commonwealth member states and non-Commonwealth states.[248]

(2) The Group of Eight (G8)

Since the mid-1990s, the Group of Eight (G8) has created working groups and issued a series of communiqués from the leaders and actions plans from justice ministers. At the Halifax Summit 1995, the Group of Seven recognized "that ultimate success requires all Governments to provide for effective measures to prevent the laundering of proceeds from serious crimes, to implement commitments in the fight against trans-national organized crime."[249] The group released 40-point set of "recommendations to combat Trans-national Organized Crime efficiently" at the G7/P8 Lyon Summit. The recommendations urged the states to increase the level of criminalization, prosecution, investigation, and international cooperation, while acknowledging in their entirety human-rights protection.[250]

At the Denver Summit 1997, the Group of Eight proposed to strengthen their efforts to realize the Lyon recommendations, by concentrating on punishing high-tech criminals, and promoting the governments' technical and legal abilities to react to trans-territorial computer crimes.[251] The Group of

248 Commonwealth Secretariat, The Harare Scheme on Mutual Assistance in Criminal Matters: Possible Amendments to the Scheme and Discussion of Interception of Communications and Related Matters, Meeting of Commonwealth Law Ministers and Senior Officials, Accra, Ghana, 17-20 October 2005. Annex 1: Summary of recommendations of the Expert Working Group, R4, p. 5.

249 G7, Chairman's Statement, 17 June 1995, Halifax Summit, 15-17 June 1995.

250 P8 Senior Experts Group, 40 recommendations to Combat Trans-national Organised Crime, Paris, 12 April 1996, Reference: 1996CIIa5.

251 G8, Communiqué, Denver, 22 June 1997, Denver Summit of the Eight, 20-22 June 1997.

Eight Meeting of the Justice and Interior Ministers of December 1997 responded to the increased international movement of criminals, organized crime, and terrorists and their use of the ICT.[252] Ministers noted, in a Statement of Principles Concerning Electronic Crime, that, while criminal legislation was a national responsibility, the character of the information networks obstructed countries from operating traditional power over this problem. Domestic legislations have to be complemented by international cooperation to criminalize the abuse of the networks and harmonize the investigative action.[253]

At the subsequent summits, the Group of Eight repeatedly expressed their concern about cybercriminality. At the Okinawa Summit, the Okinawa Charter on Global Information Society adopted the principle of international collaboration and harmonization of cybercrime. "In order to maximize the social and economic benefits of the information society", the Group of Eight agreed on principles and approaches for the protection of privacy, the free flow of information, and the security of transactions.[254]

The Charter recognized that the security of the information society necessitated coordinated action and effective policy responses.[255]

(3) The Organization for Economic Cooperation and Development (OECD)

With its 34 member countries, the OECD addressed computer security for several decades. In 1983, an expert committee was appointed by the OECD to discuss computer crime phenomena and criminal-law reform (Schjolberg and

252 December 1997, the G8 Meeting of Justice and Interior Ministers.
253 ibid.
254 G8, Okinawa Charter on Global Information Society, Okinawa, 22 July 2000.
255 ibid.

Hubbard 2005). Offences against confidentiality, integrity or availability listed in the 1985 OECD document included unauthorized access, damage to computer data or computer programmes, computer sabotage, unauthorized interception, and computer espionage.[256] In December 1999, the OECD officially approved the Guidelines for Consumer Protection in the Context of Electronic Commerce (Department of Justice 2000, p. 27), representing member states' consensus in the area of consumer protection for e-commerce: consumers should be protected in e-commerce not less than the protection they enjoyed within traditional commerce (Department of Justice 2000, p. 27). The OECD adopted Guidelines for the Security of Information Systems and Networks in July 2002, calling on member governments to "establish a heightened priority for security planning and management", and to "promote a culture of security among all participants as a means of protecting information systems and networks" (OECD 2002, Part I).

The Guidelines established nine principles, including awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, and reassessment (OECD 2002, Part III). Because of the nature of the guidelines and the distance from the legal actions, practical endeavours were left to the member countries to make.

9.6 Global efforts by the United Nations (UN)

---

[256] Computer-Related Crime: Analysis of Legal Policy, ICCP Series No. 10, 1986. Cited in UN, Crimes related to Computer Networks: Background Paper for the Workshop on Crimes Related to the Computer Network, Tenth UN Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, 10-17 April 2000, A/CONF. 187/10.

In a certain sense, there are numerous global organizations. Nevertheless, the UN is capable of being identified as the only global organization that forms a forum of its 193 member states with fuller functions. Compared with professional organizations, the UN does not limit its activities to certain domains. Compared with regional organizations, the UN does not limit its activities to certain states (in the field of cybersecurity protection and cybercrime prevention). The actions of the UN have unique advantages in coordinating international positions.

In 1985, General Assembly Resolution 40/71 of 11 December called upon Governments and international organizations to take action in conformity with the recommendation of the commission on the legal value of computer records of 1985, in order to ensure legal security in the background of the broadest possible use of information processing in international transactions.[257]

In 1990, the General Assembly of the UN adopted the Guidelines Concerning Computerized Personal Data Files. It proposed to take appropriate measures to protect the files against both natural and artificial dangers. The Guidelines extended the protection of governmental international organizations (Part B).

"The International Review of Criminal Policy: United Nations Manual on the Prevention and Control of Computer-related Crime" called for further international work and presented a proper statement of the problem. It stated that at the international level, further activities could be undertaken, including

---

257 See UN General Assembly Resolution A/RES/51/162 (30 January 1997).

harmonizing substantive law, and establishing a jurisdictional base.[258]

The Background Paper for the Workshop on Crimes Relating to the Computer Network at the Tenth UN Congress on Prevention of Crime and Treatment of Offenders proposed two levels of definition of cybercrime: In the narrow sense, that is, the strict computer crime, had to refer to "any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them." In the broad sense, that is, computer-related crime denoted "any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distribution information by means of a computer system or network."[259]

The UN General Assembly has endorsed several resolutions dealing with its desire to witness progress regarding this issue. According to information provided by SchjØberg and Hubbard (2005), checking Resolutions 55/63 (2000) and 56/121 (2001) on Combating the Criminal Misuse of Information Technology, the value of the Group of Eight Principles was noted, and states were urged to consider these principles; checking Resolutions 53/70 (1998), 54/79 (1999), 55/28 (2000), 56/19 (2001), 57/53 (2002), 57/239 (2002), 58/32 (2003), and 58/199 (2003), all calling on member states "to promote the multi-lateral consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats."[260] These resolutions

---

258 United Nations Crime and Justice Information Network (1999), Paragraph 295.

259 UN, Crimes Related to Computer Networks: Background Paper for the Workshop on Crimes Related to the Computer Network, Tenth UN Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, 10-17 April 2000, A/CONF. 187/10, p. 5, paragraph 14.

260 See UN web site.

have the same motive to improve the cybersecurity awareness at both the international and the national levels.

In Resolution 55/63, the General Assembly noted the value of the following measures to combat computer misuse:

(a) To ensure the elimination of safe havens for cybercriminals;

(b) To coordinate cooperation in the investigation and prosecution of cybercrime;

(c) To exchange information for fighting cybercrime;

(d) To train and equip law-enforcement personnel to address cybercrime;

(e) To protect the security of data and computer systems from cybercrime;

(f) To permit the preservation of and quick access to electronic data pertaining to particular criminal investigations;

(g) To ensure mutual assistance regimes for the timely investigation of cybercrime and the timely gathering and exchange of evidence;

(h) To remind the general public of the requirement to prevent and combat cybercrime;

(i) To design information technologies to help to prevent and detect cybercrime;

(j) To take into account both the protection of individual freedoms and privacy and the preservation of the capacity of Governments to fight cybercrime.

The General Assembly invited States to consider the measures in their endeavour to fight the criminal misuse of information systems, and decided to maintain the question of the criminal misuse of information technologies on the agenda of its future session.

In Resolution 56/121, the General Assembly invited states to consider the work and achievements of the Commission on Crime Prevention and Criminal Justice and of their international and regional organizations when developing national law, policy and practice to prevent cybercrime.

The resolution emphasized the value of the measures set forth in Resolution 55/63, and again invited states to take them into account in their efforts to combat the criminal misuse of information technologies. However, the General Assembly decided to postpone consideration of this subject, pending work considered in the plan of action against high-technology crime of the Commission on Crime Prevention and Criminal Justice.

General Assembly resolution 65/230 requested the Commission on Crime Prevention and Criminal Justice to establish an open-ended intergovernmental expert group, to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation.

In its resolution 67/189, the General Assembly noted with appreciation the work of the open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and encouraged it to enhance its efforts to complete its work and to present the outcome of the study to the Commission on Crime Prevention and Criminal Justice in due course.

In 2012, UNODC initiated a comprehensive study on cybercrime so as to clarify the problem of cybercrime and Member States' responses. The results were presented in 2013 (UNODC 2013). Within this Study, these topics are

covered in eight Chapters: (1) Connectivity and cybercrime; (2) The global picture; (3) Legislation and frameworks; (4) Criminalization; (5) Law enforcement and investigations; (6) Electronic evidence and criminal justice; (7) International cooperation; and (8) Prevention (ibid., p. ix).

It is necessary to mention that, besides the advantages, the disadvantages of the UN's actions are also striking. The UN is a multifunctional international organization, which in some sense has malfunctioned over the years. Focusing on the current topic, it can be said that the consensus on cybercrime in this forum remains a preliminary one. The diversified legal systems of members of this gigantic organization hinder the conclusion of a fruitful agreement.

9.7 The focuses of international harmonization

From the above presentation on international actions in anti-cybercrime areas, we can further summarize the major themes of these international organizations. These aspects mainly include the promotion of security awareness at both the international and national levels, the harmonization of legislation, coordination and cooperation in law enforcement, and direct anti-cybercrime actions.

(1) The promotion of security awareness at the international level

The typical actions in this aspect have been taken by the UN. The UN's two Resolutions (55/63 (2000) and 56/121 (2001)) on Combating the Criminal Misuse of Information Technology recalled the importance of the Group of Eight principles, and urged states to take these principles into account. Some

other resolutions also called on member states to promote the multi-lateral consideration of existing and potential threats in the field of information security, as well as promising measures to limit these threats. Other international organizations also made efforts to promote security awareness at the international level. For example, after the 9/11 incidents, the APEC Leaders called for a reinforcing of APEC activities to protect critical infrastructure.

(2) The promotion of security awareness at the state level

All international organizations have made efforts to promote security awareness at the domestic level. For example, APEC guided its member states and regions to promote cybersecurity and tackle the threats of cybercrime. APEC also conducted a project for developed states to support other states in training personnel. The Shanghai Declaration of 2002 supported measures to fight against misuse of information.

(3) Harmonization of legislation

Legal harmonization has been a major emphasis on the work of various international organizations. Harmonization in Europe started in the 1980s and a recent achievement was the Convention on Cybercrime. Other international organizations have also endeavoured to attain legal harmonization. Early in 1981, Interpol surveyed the criminal laws of member states so as to explore defects in the existing legislation, and made efforts to harmonize the laws. Today, Interpol's African Working Party on Information Technology Crime Projects is trying to persuade the African states to sign and ratify the Convention on Cybercrime. APEC also took steps to survey the laws and to encourage economies to enact comprehensive laws consistent with the Convention on Cybercrime and the pertinent UN resolutions. The EU Framework Decision of

2002 specifically granted the member states the responsibility of criminalizing the offences of illegal access to and illegal interference with information systems. The REMJA urged states to criminalize cybercrime and harmonize the member states' laws, and consider the possibility of joining the Convention on Cybercrime. The Commonwealth Model Law on Computer and Computer Related Crime expanded the criminal liability of the Convention on Cybercrime so as to include reckless liability. Through this Model Law, the Commonwealth made efforts to criminalize cybercrime in the member countries. The Group of Eight Paris Conference discussed the public and private interact with the objective of implementing an international penal code for fighting cybercriminality. The Okinawa Charter on Global Information Society further consented to international collaboration and harmonization concerning cybercrime.

(4) Coordination and cooperation in law enforcement

Interpol's European Working Party on Information Technology Crime compiled the Computer Crime manual to provide technical guidance in law enforcement. The Convention on Cybercrime also covers cooperative mechanisms in law enforcement against cybercrime. The EU discussed about the retention of traffic data in 2001. The Ministers of Justice or Ministers or Attorneys General of the Americas (REMJA)'s Group of Experts on Cybercrime have been devoted to discover cooperation ways in the Inter-American system to combat cybercrime. The Group of Eight reviewed existing cooperation mechanisms and gaps, and made attempt to discover ways to fill these gaps. The Group urged the states to increase criminalization, prosecution, investigation, and international cooperation. The Denver Summit proposed to

promote governments' technical as well as legal abilities to act in response to trans-territorial computer crimes. The Birmingham Summit called for agreement on a legal framework for evidence preservation and protection of privacy, and for agreements on the international sharing of evidence so as to struggle more effectively against a broad scope of crimes, including cybercrime.

(5) Direct anti-cybercrime actions

The direct international anti-cybercrime actions comprise two fundamental aspects: cybercrime prevention and cybercrime investigation. They have been more valuable before international harmonization in legislation could come into being. Different organizations have taken individual measures with specific emphases. For example, Interpol directly cooperated with credit-card companies to fight against payment fraud. The OECD's Guidelines for Consumer Protection in the Context of Electronic Commerce 1999 emphasized the protection of consumers in e-commerce as well as that in traditional commerce. Guidelines for the Security of Information Systems and Networks 2002 called on member governments to "establish a heightened priority for security planning and management", and to "promote a culture of security among all participants as a means of protecting information systems and networks".

9.8 From conversation to the European Convention

As one of the most outstanding achievements, international actions bred a comparatively effective implementation: the Convention on Cybercrime and its Protocol. The general purpose of the Convention is laid down in the Preamble

as to deter crimes against the confidentiality, integrity and availability of information systems and the misuse of such systems. The purpose of the Protocol is to supplement the provisions of the Convention on cybercrime on the criminalization of acts of a racist and xenophobic nature committed through information systems (Protocol, Article 1).

The Convention has been widely accepted as a landmark, providing for both the substantive and procedural legal frameworks, both the domestic and international level of countermeasures, so as to achieve higher effectiveness in fighting against cybercrimes.[261]

Articles 2-12 of the Convention have required nations to criminalize the activities of illegal access to data and computer systems; illegal interception; data and systems interference; misuse of devices that can be used to enact the aforementioned crimes; computer-related forgery and fraud; content-related offences including child pornography; copyright crimes; and attempt, aiding or abetting. Article 13 of the Convention also establishes corporate liability, and sanctions and measures for these offences. Articles 3-7 of the Protocol requires nations to criminalize the activities of disseminating racist and xenophobic information through information systems. Also to be criminalized is racist and xenophobic motivated threat, racist and xenophobic insult, and in respect of genocide or crimes against humanity, denial of their existence, gross criminalistic approval or justification of them, and the behaviour of aiding and abetting them.

The Convention provides two constituent elements for cybercrimes. First, the Convention establishes criminal liability on the subjective element of intent.

---

[261] Convention on Cybercrime, Preamble, Paragraph 9.

Sometimes, the constitution of certain offences requires elements such as intent to procure "economic benefit" in computer-related fraud provided by Article 8. Second, the Convention establishes criminal liability on the objective element on act "without right" in all offence provisions.[262] The problems of what is an act committed intentionally, what is an act with right and without right, are all left to national law interpretation.

The Convention allows domestic laws to provide additional constituent elements, and provides the possibility of a reservation.[263] Apparently, the Convention fully respects the decision-making of member states on the matter of criminal policy. As a result, we have good reason to worry that this diversified implementation will decrease the consensus on the harmfulness of conducts and increase the possible obstacles to international actions. The negative effect of this kind of provision is expected to diminish the effectiveness of prolonged expensive international negotiation for an agreement, although the provision itself is exactly one of the contents negotiated and agreed upon.

The Convention has also been criticized by civil liberties groups concerned that it will undermine individual privacy rights and that it expands too greatly surveillance powers, and is fundamentally unbalanced. As Taylor (2004) pointed out, the Convention contains comprehensive, far-reaching powers of surveillance, search, and seizure, while lacking a criterion for the protection of privacy and limitation of power.[264] The basic concerns in the field

---

262 Convention on Cybercrime, Articles 2-12.
263 Ibid, Articles 40 and 42.
264 Taylor, G. The Council of Europe Cybercrime Convention: A Civil Liberties Perspective, 23 July 2004. Retrieved 15 February 2016, from http://crime-

of human rights are the over-expansion of the states' power of surveillance, and over-criminalization of citizens' behaviour. Before information systems have been completely developed, the states would strictly take this borderless system under control; those who use information systems would voluntarily enter the tight legal encirclement. For those who use information systems before these legal instruments, they are to accept externally imposed constraints; while for those who use information systems after these provisions, they are born into an inherent limitation. Both these two groups of users may feel a loss of freedom of information.

Despite the anxiety mentioned above, the Convention has unquestionably had some influence on the worldwide consensus in relation to the predicament of cybercrime. We are capable of seeing that the Convention will become one of the important steps towards a broader international accomplishment.

Firstly, some countries have taken practical measures to ratify the Convention. The total number of ratifications and accessions is 47 countries, including one non-member state of the Council of Europe, the U. S., with 7 countries (including one non-member states of the European Council, South Africa) having signed the Convention, not followed by ratifications.[265] The treaty has entered into force in only a small number of countries, representing a small proportion in terms of land area and population. However, it is still an important step towards a broader consensus: "A little is better than none."

Secondly, besides successful endeavours, countries, including most signatory countries, are still on their way to ratifying the treaty. The Council of

research.org/library/CoE_Cybercrime.html

265 See Council of Europe, Convention of Cybercrime, CETS No. 185, Chart of Signatures and Ratifications, 13 October 2015.

Europe Conference on "Cybercrime: a Global Challenge, a Global Response" in 2005 "strongly encourage States to consider the possibility of becoming Parties to this Convention in order to make use of effective and compatible laws and tools to fight cybercrime, at domestic level and on behalf of international co-operation."[266] The treaty has come into force in some of the Nordic countries, including Denmark, Iceland, and Norway, but Finland and Sweden are still seeking ratification though they were both countries of signature on the date opening for signature in 2001.[267]

However, this process has proved hard without the expected number of countries ratifying in the five-year period after the Convention was open to signature. The pressure against not ratifying the treaty coming from inside the countries seems to be a greater obstacle than the differences over the drafting of the document. A significant obstacle comes from the difference of legislative styles between the Convention and the individual countries. Many of the valid provisions in current Finnish law do not need revision.[268] Whether the original Finnish Penal Code (which includes quite a few revisions concerning offences relating to data processing) is capable of dealing with *all* of the offences provided by the Convention has not been tested in judicial practice. But the Finnish legislature will have to add some new provisions to the Penal Code, if it wants to cope with the Convention. Expressly, provisions

---

266 Council of Europe, Conclusions of the Council of Europe Conference on "Cybercrime: a Global Challenge, a Global Response", Madrid, 12-13 December 2005.

267 See, for example, the Governmental Proposal HE 153/2006 of Finland, which aims at bringing the Convention on Cybercrime and the European Union's Framework Decision on Attacks against the Information System into force in Finland and making relevant revision in domestic provisions according to the Convention (HE 153/2006, 3. Objectives and Central Proposals).

268 HE 153/2006, Detailed Justifications.

concerning the offence of interference with and gross interference with the information processing systems, the offence of possession of instruments for cybercrime (covering the computer viruses), the liability for inchoate cybercrime, and for corporate liability, and so forth must be taken in.[269]

The critical challenge of the Convention on Cybercrime to conventional international legal cooperation lies in the absence of a demand for the double criminality criterion. Since this criterion is in decline, individual countries are far from implementing it in domestic law, either. In accepting the Convention, individual countries will therefore have to revise domestic laws in the relevant area.[270]

Some other countries are seeking to remodel the Convention so as to provide a prohibition on the types of conducts and to create procedural and international mechanisms for serving successful investigations and prosecutions of crimes. The flexibilities of the Convention may have a positive effect in leaving to member states the alternative of using different methods and languages in their domestic law. This may actually lead to a wider application of the Convention so as to cover more and diversified legal systems. While the U.S. has asserted that its own domestic law dos not need revision, South Africa has implemented substantial criminal provisions in line with the Convention. Japan is considering filling the gap between its domestic law and the Convention. At least, among the APEC economies, Taiwan, the Philippines, and Hong Kong are considering taking the Convention as the basis on which they will carry out their own legislative amendments.

---

269 HE 153/2006, General Justifications, 3. Objectives and Central Proposals.
270 ibid.

Some international organizations are propelling cooperation in promoting the member states' access to the Convention. As mentioned above, in the framework of Interpol, the African Working Party on Information Technology Crimes is working to promote domestic legislation and adherence to the Convention. APEC, the EU, and the REMJA V of the OAS have also taken measures to spread the Convention to its member states.

There are also efforts to develop cybercrime legislation beyond the Convention. As mentioned above, the Commonwealth's model law represents a breakthrough in extending criminal liability to the *mens rea* of offences of interfering with data, interfering with computer systems, and illegal devices so as to include reckless liability. Some of the Commonwealth's member states are also on their way towards legislation that will model the Convention and model domestic law.

Finally, in fact, most countries, particularly countries where cybercriminals are usually left at large, have taken no action in spite of the importance of the Convention. These countries have very specific interests in maintaining what may be considered "criminal" in other countries but are "legal" in their own countries, as far as web sites, services, or even sales of goods online are concerned. The potential cybercrime perpetrators, regardless of whichever nationality they belong to, also seek asylum in such countries in order to escape punishment by countries that are seeking to extend their judicial arms to deal with cases committed inside their sovereign territory and committed by their citizens outside their territory.

Although the Convention on Cybercrime has been attracting increasing attention at both the domestic and international levels, it is necessary to point

out that, once the Convention was in documentary form, the enthusiasm and efforts of other international entities towards a higher degree of international harmonization of legislation have been to some extent weakened. This situation reflects neither the purpose, nor the intended side effect of the Convention. However, a ready instrument must have its negative influence on the otherwise unsettled disputes of the problems of cybercrime deterrence. Regrettably, both the advantages and disadvantages of the Convention will bring about a more cautious discussion and a better plan will be discouraged from being implemented. At least, the similar but different schedules for international treaties, in either broader or narrower scope, have seen an interruption with the passing of the Convention. The Convention thus becomes not only a mutual compromise of member states, but also a turning-point in the knowledge and experiences of cybercrime punishment and prevention.

Traditionally, new legal instruments have usually been the subject of academic annotation immediately after its implementation, while the legislature is usually reluctant to change existing legal instruments. These two factors further determine the unfortunate fate of the better and newer proposals, particularly proposals having more or less better elements than the implemented one. In a word, we can say that classics were good, but classics hinder better classics; consensus is good, but current consensus always hinders better consensus: and the current Convention is good, but an existing convention potentially hinders a yet better convention.

Although the Convention was also appraised by politicians, such as the U. S. President George W. Bush, as "providing for broad international cooperation in the form of extradition and mutual legal assistance", and containing

"safeguards that protect civil liberties and other legitimate interests" (Bush 2003), the effectiveness of the Convention's cooperative framework is subject to reasonable doubt without a majority of countries' access to the agreement (Goldsmith 2005, p. 4). Authors such as Archick (2004) have proposed that the Convention's arm would not be long enough to reach the countries that are regarded as a "haven" for cybercriminals: attacks are launched from those countries, but the countries do not join the agreement. Consequently, the countries with law and without law, or being the member and being non-member of the Convention, have to encounter mutual conflicts. The situation confronting international society is obviously still one of the tardiness of the acceptance of existing instruments and the lack of a universal agreement.

9.9 Limited progress in international harmonization

Over the years, the international co-operation on cybercrime "has been very active and comprehensive" (Pihlajamäki 2004, p. 286). The international level of consensus on criminal law has, however, not been achieved. Previously, the criminalization of war crimes, crime against peace, crimes against humanity, genocide, torture, and other crimes have been the successful examples. The application of pertinent agreements in specific courts has demonstrated that an international forum can acquire certain achievements prior to legislation at the national level. Traditional international criminal law has aimed at harmonizing substantive law and coordinating procedural law on offences that have existed in

society since the coming into being of humankind.[271] Presently, what the countries are eager to realize is an international agreement on offences with a history of only several decades. The anxiety for success, the absence of trial practice, the lack of an accumulation of experience and knowledge, the alienation between the legislature and general public, and the different interests between the various countries, all deliver an international consensus in its lowest form. It is inevitable that during the drafting stage and particularly after the Convention on Cybercrime has been opened for signature, many commentators have published their evaluation and criticism.[272] Combined with other progress made in international harmonization, the most important unsolved problem may be the limited participation and the limited consensus.

Firstly, international harmonization has hitherto been primarily the forum of the developed countries. The working mechanism of an effective international treaty is for all of the signatory countries to take effective action and preserve a common theatre of operation. The treaty is not aimed at any third party and thus the third party is not restrained by it. The participating countries of the Convention on Cybercrime are limited, representing only a limited population. Along with the development of the Internet globally, the number of cybercrimes will be correlated with the population base of Internet penetration, and the global population base. Most of the present international harmonization measures have not been incorporating the countries with the largest population. This will make the measures less effective. Considering the

[271] The origin of human beings has been an unsolved theoretical problem. Genesis theory and evolutionary theory might be the most influential arguments.

[272] For an overall evaluation on the Convention on Cybercrime, see Jones (2005). The Convention was also subject to criticisms from individuals and organizations, such as the American Civil Liberties Union and others.

characteristics of cybercrime, the "safe haven for criminals" can only be eliminated when almost all the sovereign states have access to one agreement and almost all the online users are subject to the power of law enforcement. Although an international document can be modelled by member states when making domestic laws, the expectations should not be raised too high in respect of a timely update at a similar pace when it comes to international measures.

Secondly, another limitation is that a lower level of consensus has been reached. Unlike traditional offences in international criminal law, which have rarely been penalized in domestic law, cybercrime was initially devised in the legislation at the national level. In many countries, domestic legislation on offences such as genocide, crime against peace and similar types of crime did not happen before the countries were subject to the obligation of international treaties. The situation of cybercrime is that countries that have already enacted laws assisted or forced the countries that have not enacted laws to enter a consensus. As a whole, international cooperation in preventing cybercrime is more sluggish than domestic legislation; its impact on domestic legislation is, nonetheless, undeniable. Domestic laws should be amended according to international instruments so that the measures provided in the international instruments can be effectively carried out. An agreement on a wider scope of issues in cybercrime is also necessary so as to ensure effective law enforcement. However, such an agreement is still lacking. The efforts of various international organizations should be integrated into a more unified action.

Thirdly, there is, strangely, a tendency towards pluralization on the international harmonization. In regulating or deregulating the information community, different interest groups stay at different standpoints. In

criminalizing and decriminalizing the online activities, different players hold different opinions. Different organizations propose countermeasures for the benefit of a certain number of their member states. Yet other organizations oppose any kinds of plans for imposing constraints on the free use of information systems. The mechanism is that while one interest group is anxious about the misuse of information systems, another group may concentrate on the side-effect of anti-misuse actions. Various international harmonization measures are full of a trade-off of interests and a contrast of powers. This marathon process of negotiation has inherited the inherent style of international actions.

Fourthly, another tendency is the regularization of international harmonization. The effect of international harmonization is less significant compared with the efforts. The role of the UN as a universal international organization seems limited to arranging an international treaty in this area. If the United Nation's frequent "call" does not motivate member states to legislate on cybercrime, a universal agreement would be a better alternative in promoting consensus. The UN may have the opportunity to incorporate the consensus reached in other fields into the above-mentioned unified action. By doing so, traditionally soft international cyber law can become a realistic platform for international discussion, can acquire stronger force in international legislation and law enforcement, and can have more say in facilitating international consensus and promoting international cooperation.

9.10 Conclusion

Globalization does not mean globalized welfare at all. Globalized information systems accommodate an increasing number of trans-national offences. The network context of cybercrime makes it one of the most globalized offences of the present and the most modernized threats of the future. We can take actions in two different ways to resolve this problem. One is to divide information systems into segments bordered by state boundaries. The other is to incorporate the legal system into an integrated entity obliterating these state boundaries. Apparently, the first way is unrealistic. Although all ancient empires including Roman, Greece, and Mongolia became historical remnants, and giant empires are not prevalent in current world, the partition of information systems cannot be an imagined practice. Information systems become the unique empire without tangible territory.

Offences occurring in information systems are not likely to receive punishment from this system. Rather, they are punishable by the territory-based states that they cross. It is increasingly stringent and necessary to establish an international cooperation system for punishing cybercrime. Various international organizations have taken actions to resolve the problem in different forums and at different levels.

The Convention on Cybercrime is acknowledged as a landmark in the sphere of the international harmonization of cybercrime law.[273] However, apart from the fact that it represents a significant step forward, more states will have to sign the Convention and abide by its mandates in order to serve as a deterrent. International harmonization centred on the Convention is obviously

273 See the Council of Europe Cybercrime Conference, Conclusions, 15-17 September, 2004 High-level Conference on the Challenge of Cybercrime.

limited and must necessarily be extended to more participating member states with an even wider scope of issues. The final effect should be achieved only through a universal agreement on combating cybercrime. The UN may have higher potential to implement such universal measures. However, we should not expect an instantaneous reaction from any of the international organizations, because not too much attention and interests of these international organizations are concentrated on the problem of crime or precisely, on cybercrime. While these organizations are devoted to dealing with the more important international affairs, threats against a critical information infrastructure will become more serious, until they are listed at the top of these organizations' schedule. Consequently, the development of an international level of consciousness and an international level call for a national level of consciousness are still the grounds for effective actions. The need is to reassess and renew as necessary the present international legal frameworks, offering a forum for broader international discussion expressing an outlook towards increasing and advancing international law-enforcement cooperation among the national authorities. This development should consider the influences of the novel and emerging issues in respect of international law-enforcement cooperation, with recommendations on capacity-building, which should show an equal concern for the situation in countries at different stages of development so as to avoid a futureless future of information chaos.

CHAPTER 10 CONCLUSIONS

10.1 Dilemmas of cybercrime control

The possibility of disseminating information in large quantities and at high speed serves both legitimate and illegitimate purposes. Cybercrime can be seen as a by-product of cyberspace, which is the product of information and communications technology. Twenty-first century witnesses an increasing tendency of offenses heavily relied on the Internet and high technologies to promote their malicious activities. The current information systems are insecure systems, while the present Internet is an insecure network. Crime is a phenomenon that easily emerges but is difficult to eliminate. The phenomenon of cybercrime is the silhouette of the information society. The Internet services lack of controllability and become the breeding ground of cybercrime, as a response to which many governments have enacted specific legislation criminalizing invasive and destructive activities targeted at information systems. Because cybercrime, committed with the assistance of the globally-connected computer networks, can easily cross the territorial borders, it is unknown but broadly accepted that different countermeasures may create a paradise for cybercriminals. Great challenge has been posed for cybercrime control

(Grabosky 2000, pp. 9-16). Consequently, a critical step will be the elaboration of common international rules concerning these crucial factors so as to fill the legislative and jurisdictional gaps.

Technology should be the preferential choice for eradicating cybercrime. Cyberspace can be considered as the expansion of society, while cybercrime is the extension of criminal phenomena. Although cyberspace is not entirely independent, there is the possibility and even necessity for autonomy within the independent factors. Technicians are constantly inventing technological countermeasures to deal with issues of cybersecurity, but an increasing number of commentators argue that the techniques of security cannot keep pace with techniques for discovering loopholes in information systems and for launching attacks on information systems. It is impracticable to solve the whole problem merely by the means of technology.

To some extent, cybercrime mobilizes law. Criminal law and other laws, professional codes, industrial self-discipline and user ethics form guidelines, though their functions are quite varied as between the different countries. Most of the modern democratic countries do not exploit penalties as primary means for correcting human behaviour. Criminal law remains the main tool. However, if criminal law cannot respond to the reality of crime, if law cannot be enacted to impose a suitable liability on harmful activities, and if law cannot be enforced by qualified personnel, the law will unquestionably be ineffective. In fact, in the current technological environment, legislature and law enforcement can hardly adjust their activities in response to the new situations. Criminal law becomes a law the principle and stability of which hamper its inherent functions. We must point out that, this is possibly contrary to the nature of law.

Even some high-profile law-enforcement officers can fail in detecting offences, or misuse their posts to serve political ambitions, or fabricate fictitious cases. As some of their failure and misconduct become better known, the placing of trust in them will be accompanied by great risks. Apart from this concern, law-enforcement agencies, even in normal situations, have found that it is much more complex to detect, investigate, and convict cybercriminals than traditional criminals. In the networked world, it has become increasingly uncomplicated for criminals to avoid conviction by acting from a country where a conduct is neither criminalized nor prosecuted. International cooperation and legal harmonization are necessary for reducing investigation costs and increase enforcement effects. The Convention on Cybercrime is therefore used by governments in order to harmonize their cybercrime laws and increase cooperation and coordination between national law enforcements agencies. However, there is an especially long road before perfect harmonization is achieved. Unification of substantive criminal law, harmonization of jurisdiction, coordination, and cooperation in cybersecurity protection and cybercrime prevention, will all contribute to lower the cost of deterrence.

As we mentioned above, the insufficiency of the existing legal framework and the inefficiency of detection and conviction imply that high costs will be involved in cybercriminal law enforcement. Seneca stated that: "He who does not prevent a crime when he can, encourages it." (Lucius Annaeus Seneca, Troades CCXCI) The problem at present is: "He who does not prevent a crime when he cannot, also encourages it." In addition to the technological obstacles, the limits imposed by state borders and the difficulties in establishing

international cooperative mechanisms render it burdensome to combat cybercrime effectively. The low quality of law and its enforcement finally results in injustice and inequality, destroying the long established principle of legality. An inefficient and ineffective legal framework for control over cybercrime will run the risk of creating new unfairness in the information age. The information society does not definitely lead to a harmonious world. Although pervasive information enables people of all circles to be more informed, and to work more efficiently and more effectively, it raises multiform questions. The distributive disequilibrium of information of various values between groups results in unbalanced power of control as well as anti-control forces. The deficiency of law and the prevalence of lawlessness may become two of the most notorious negative factors.

From the standpoint of the above analysis, a worldwide unified model of substantive and procedural cybercriminal law would be very ideal but not so much practical. Regional international cooperation has a better foundation and can be used to improve the legislation of participating member countries. Negotiation and cooperation among the developed, developing and transition countries provide the most important forum for eliminating the refuge for cybercriminals.

The above discussion implies that law is not likely to be perfect. At the same time, we must also note that even if there is perfect law, it is not the perfect solution. Law must be enacted by some persons against some other persons. The absence of either a subject or an object in law enforcement would leave the law ineffective. Law enforcement has also frequently been disappointed with the effect of traditional crime prevention. The situation of

cybercrime has nothing more special than its traditional counterparts in improving the prevention effect. Criminals have escaped detection regardless of the existence of law and of the police. We can be convinced by many findings and conclusions about traditional crime control programmes, for example, the situation in the following comments described by Duckett:

"Gun control has not worked…The only people who have guns are criminals. We have the strictest gun laws in the nation and one of the highest murder rates. It's quicker to pull your Smith and Wesson than to dial 911 if you're being robbed." (Duckett, Washintong Post, 22 December 1996)

Particularly, the private sector of the information society should not wait for any external remedies for their cybersecurity. Direct and instant approaches to protecting their information assets and online business is self-protection, upon which coordinative and cooperative mechanisms can be used as the *ex post* remedies. Practically, the function of judicial activities is to inflict liability on parties involved in the creation of insecurity, even though the supposed general deterrence of penalty can also forestall potential criminals from behaving detrimentally.

Neither laws nor technologies can do everything that people normally expect, even in their duties. The more appropriate strategies for the control of cybercrime require an arrangement of law enforcement, technological and market-based solutions. Obviously, even if we combine all these measures, the problem would still not be solved. This recognition has become a consensus among cybersecurity and cybercrime researchers. For example, McConnell International (2000, pp. 1 and 7) stated that "self-protection" is inadequate to secure the cyberspace, and the law is necessary to play its role; however, "law is

only part of the answer." These dilemmas of maintaining cyberspace order necessitate the adoption of comprehensive measures. Pamela Samuelson (1989) mentioned that: "The law may not be the most precisely sharpened instrument with which to strike back at a hacker for damages…but sometimes blunt instruments do an adequate job." Law in itself will hardly be able to act as complete substitutes for security measures. The law will hardly have enough deterrent power if the majority of people are unaware of its range and sense. Cybercriminals habitually consider that they are problem-solvers other than lawbreakers (Leiwo 1995, p. 50). The traditional hacker even thought the supposed "freedom of information" means that all the computers and networks should be open to every user. Under their codes, rules or ethics, the legal framework that traps the unauthorized intruders in information systems becomes an injustice. To awaken public awareness and consciousness concerning privacy and security, the task falls on the shoulder of education, and the market. In the end, all these measures are necessary, but none of them can work in an optimistic manner alone.

10.2 The primary factors benefiting cybercrime

From the analysis and discussion in this book, it is possible to draw several fundamental conclusions on why cybercrime exists and spreads. The explanation on the causes of crime has produced many criminological theories. Grabosky, Smith, and Dempsey (2001, pp. 2-3) turned to Cohen and Felson's routine-activity theory (1979) and described an online presence of motivated

offenders and suitable targets, and online absence of capable guardians. The factors involved in the dynamic interaction of cybercrime and the peripheral environment may be even more numerous. The opportunities for crime, the motivation of criminals, and lack of deterrence make it safer to commit cybercrime than traditional crime, and make it more beneficial to commit crime than to be engaged in legal occupation. I consider the following as the primary causal factors of the above phenomenon:

(1) Cybercrime is the natural extension and irresistible tendency of criminal phenomenon in information systems. To explore the reasons why there is cybercrime, it is inevitable to identify the root causes and evolution of crime. Crime has existed since ancient times, will exist eternally, but its nature changes along with the development of society. Wherever there are human activities, there will be deviances. As Radzinowicz and King pointed out:

"No national characteristics, no political regime, no system of law, police, justice, punishment, treatment or even terror has rendered a country exempt from crime." (1977, p.3)

Information systems have been integrated as an inseparable part of society, and the traditional social problem will surely settle down in the new world. The inevitable fate of information systems can be expected to be similar to all the previously existing new worlds in human history. Although types of crime may be different from each other, criminality will develop together with an increase in criminal utility. In an information society, crimes are naturally symbolized by information. These crimes are committed using information systems, abusing information systems, and through information systems. The new crimes inherit the genetic characteristics of the old crimes, even though these characteristics

may evolve and change. Cybercrime is the product of the evolution and change in traditional crimes, being a component of the changed criminal system, but not a brand-new creation. People should be neither frightened nor be unprepared for such a natural historical phenomenon.

(2) Cyber transgressors and criminals lack a sense of guilt. The lack results from both internal and external factors that distort value judgement, that is, the perpetrator's and the public's ambiguous attitude towards such activities. Bequai (1983, pp. 70-84) brought forward the viewpoint of "lack of ethics as a cause of crime," criticizing society's "glorifying the computer criminals" (p. 72). Cornwall (1987, pp. 134-137) discussed the "lack of moral clarity" in the whole white-collar crime. From this aspect, though not all cybercrimes can be categorized as white-collar crimes, they have a similarity to white-collar crime. Cyberspace is a virtual world, in which there is a lack of social supervision over all conducts; it is in a hidden environment and one that is difficult to trace back. At the same time, the police remain blind to cybercrime to a great extent. Many perpetrators are even proved to think that the crimes they commit using the Internet represents their high intelligence quotient. In addition, there are the cases where virus authors and hacking perpetrators are praised and even hired for key positions in the information security industry. All this misinformation regarding virtue and vice removes the sense of guiltiness of the transgressors and criminals, stimulating the criminal mind, obliterating security and insecurity, and confusing the right with wrong. Under the control of this kind of consciousness, people are willing to engage in criminal actions, unlike most of us whose mental status is against any apparent deviance. Decency and deviance are contradictory orientations.

(3) Many users have a strong curiosity to access information systems and an intense desire for self-manifestation. When the U. S. computers were attacked by Morris, it was recognized that "government and commercial experts were less prepared to deal with the worm invasion than were students" (Marshall 1988, p. 1121). In order to maintain information security, most networks are permitted access only to those authorized or to registered users. The unauthorized users are denied access through identity and password checks and other access-control mechanisms. However, this often touches the very thing that inspires common human nature –curiosity. In the face of the data that hackers cannot access, they develop malicious programmes to intrude into the unknown field, or they crack the passwords to probe into the closed space driven by curiosity. By cracking the networks defence and accessing information systems, they demonstrate the high level of their technique, and considering this process as an intelligent challenge.

(4) The low cost of cybercrime and the difficulty in detection and evidence collection create incentives for potential perpetrators. The nature of high intelligence, trans-territoriality, and high concealment of cyber transgress and cybercrime make it difficult to detect and investigate the cases (See Conly 1991; Clark 1996; Stephenson 2000; Mandia and Prosises 2003; Mohay and co-workers 2003; Vacca 2005; Johnson 2006). Stating from another standpoint, cybercrime surpasses the current capacity of public and private regulators to control (Grabosky 2000, p. 2). As for the transgressors or criminals, they usually only need to click the mouse or knock the keyboard at home or in the office in order to commit the illegality in a short time. The risks and costs are in cybercrime lower than those in traditional crime, while the benefits are higher.

This cost-effectiveness further strengthens the mind of the perpetrator to commit cybercrime.

(5) A lag of cybersecurity legislation diminishes the striking force against cybercrime. From the early days, scholars have recognized the importance of legal countermeasures. "The problem of computer crime is, in great part, the failure of our laws, jurists, lawyers, and law schools to adapt to the needs of a changing environment." (Bequai 1978, p. 197) Particularly, "the legal establishment has shown a reluctance to meet change." (ibid.) Due to the mere absence of legislation, many famous hackers never received corresponding punishments. Some others were questioned or even detained for some time before no law can be found appropriate to convict them. There is no universal international consensus on what exactly cybercrime is, and who has the capacity to exercise jurisdiction. Meanwhile, cyber police have been established only in recent years, and law enforcement is still at the testing-stage. In addition to the legal gap, the weak punishments help minimize prevention (McConnell International 2000, p. 8). For many scholars, more severe penalties are the definite choice for strengthening deterrence, but still others doubt whether it will be the correct "answer" for the liability of virus authors (Vamosi 2003). These doubts diminish the striking power against cybercrime, and further reinforce the criminal mind of those perpetrators.

(6) The insufficiency of cybersecurity management leaves a backdoor for possible intrusion. Traditional business security measures were designed to safeguard premises physically and deter perpetrators psychologically, ranging from restricted accessibility, removal of outside visibility, and reducing escape possibility, particularly guarding the target outside of business hours (Aromaa

and Laitinen 1994, pp. 47-101). Since the management was changed from manual to automatic, management consciousness and methods have fallen behind the development of information systems. The absence of vigilance (Bequai 1978, p. 15) may derive from the fact that individuals and organizations think more about benefits, the convenience and development of the business than of security management. The capital and human resources invested in security maintenance does not furnish the necessary safeguard. The unauthorized disclosure or acquirement of confidential information may be achieved through a "compromised storage, handling or disposal of computer devices or electronic data media," regardless of the availability of security safeguards and awareness of governments and businesses about their responsibility for protecting the security of information.[274] In addition, we never deny the technological involvement of various kinds of cybercrimes, but we also think that there is some truth in the conclusion that Felson (2002) came to:

"Most computer fraud is traced not to brilliant hackers but rather to those who leave their passwords on top of the desk with their office doors open, or who dump the technical manuals in the trash bin, or who used to work somewhere and still access information they shouldn't." (p.175.)

---

[274] Sale of Provincial Government Computer Tapes Containing Personal Information, Re, 2006 CanLII 13536 (BC I.P.C.). In this case, personal information was at risk simply through the sale of government assets, among which were 41 computer tapes containing thousands of highly sensitive records, including medical conditions such as HIV-positive diagnosis, mental illness and substance-abuse, thousands of individuals' names with social insurance numbers and dates of birth, details of applications for social assistance, and caseworker entries divulging extremely intimate information about people's lives. Besides, about 22 sold hard drives had not been wiped away, with government data accessible. All this happened due to simple mistakes made in good faith by individual government employees.

(7) Loopholes in the computers and networks technology expose the system to attacks. No operating system is hacking-proof. The malicious programmes exploit the loopholes of the operating systems and launch attacks. The security measures are often falling behind the activities of the loophole-seekers. In addition, sometimes the users do not instantly apply security measures. These factors can be summarized as the problem of computers and networks technology. Thus as the critical factor of modern society, information systems become the vulnerable target of modern crime. The need for security (Bequai 1978, pp. 19-24) remains a critical element in safeguarding information systems.

(8) The Insufficiency of family and school education and discipline grants juveniles more opportunities to abuse computers and networks. In cyber transgress and cybercrime, juveniles constitute a critical proportion of the perpetrators. The prevalence of computers, the Internet, and their use in the home create for parents the important task of teaching juveniles to use computers and the Internet correctly. In many countries, parents are important figures for the education of their children. But, if many parents do not have much computer knowledge when they buy computers for their children, children lose parental constraints. Then, the use of computers is an absolute freedom and results in cybercrime. To some extent, nonetheless, the families and schools can prevent children from perpetrating cybercrime and being victimized in the first place.

(9) The functional weakening of traditional social communication disorganizes the traditional interpersonal relationship by seeming to require instant communication. The theory of social disorganization has been used to

explore deeply into social communication (Mowrer 1942; Elliot and Merrill 1961). Social disorganization may be the consequence of many factors. We think that there is a basic reason behind the numerous factors, that is, the abundant available information in urban and urbanized regions. Traditionally, the necessity for strong interpersonal communication results from scarcity of information. But nowadays the residential concentration in an urban area or urbanized area, the development of electronic media and telecommunications devices, and the dissemination of free information by various means are meant to solve the problem of information scarcity. Under such circumstances, the acquirement of information traditionally through interpersonal communication becomes insignificant. Upon meeting the need for such information, curiosity drives the Internet users to access more information from the international information systems. With the enlargement of the incompact online community, the size of the compact offline community is shrinking. The vanishing real interpersonal communication and the emerging virtual interaction will reconstruct the form of the community and the criminal types that dwell in it. Cybercrime is one of the problematic outcomes of this reconstruction.

(10) The historical absence of restraint on white-collar employees creates a temporary opportunity for insider crime. Although the conception of white-collar crime has a history of several decades since Sutherland, public opinion on crime remains focused on violent crimes. The direct result from the conventional notion is that white-collar crime is a smaller concern in criminal justice than violence. With the deepening of urbanization and the spread of information, white-collar digital crime is exploiting the priority to deduce their guiltiness. The basic supposition is that information security breakers have been

driven by noble-minded motives and have disdained to cause harm, and consequently that even where they do cause harm, people have conjectured that they are not deliberate and selfish. Involuntary judicial neglect, media misleading, and public connivance accelerate the growth of white-collar cybercrime.

Any inquiry would be limited in scale and in result. However, we have recognised that the development of the technical network has had great impact on the social network, both positively and negatively. While the positive impact tends to strengthen social integration, the negative impact impels the disintegration of the society. The two different forces are rewriting social phenomena and the social problem. The changing social environment may have quite a few problems in coming to term with cybercrime.

10.3 The primary factors preventing cybercrime

"It is better to prevent crimes than to punish them." (Beccaria 1764, Chapter 41) Prevention of cybercrime is, however, not as simple as typing some commands on a keyboard to commit it. Grabosky (2000) recognized that cybersecurity would depend on efforts of a variety of institutions and self-help by likely victims (p. 2.). Until now, there has not been a unified set of effective measures, although many individuals and organizations have proposed numerous recommendations, mostly composed of factors similar to each other but with different emphases, such as CoE Recommendation No. R (95) 13

(1995),[275] UNCJIN (1999), McConnell International (2000), APEC (2002), etc. McConnell International (2000, pp. 8-9) made its recommendations in three categories: firms should protect their networked information, governments should enact their cybercriminal law, and firms, governments and civil society should cooperate to reinforce the legal infrastructure for cybersecurity. Recognizing that there has never been and will never be a panacea to deal with criminal phenomena, there are some factors that cannot be ignored in anti-crime actions. In contrast to the previous propositions, I shall emphasize the development and maintenance of secure information systems, promoting information ethics and law-abiding consciousness, and creating sufficient legal incentives and remedies.

(1) The developing of information systems with a higher quality

The development of a secure system is a preferential choice among all countermeasures. Just as a healthy person can resist diseases, perfect information systems cannot be victimized. However, the perfect system does not exist just as no one is perfectly healthy. In strict scientific terms, it is not possible to demonstrate a cut-off point between security and insecurity. The higher level of security is generally viewed as security, while the lower level of security is generally viewed as insecurity. Most cybercrimes relate to the defects of the systems. Insecure information systems are like defective products or services, for which the producers or providers should be regulated by the law on product-quality control. Secure information systems can be acquired through

[275] Council of Europe Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information Technology (Adopted by the Committee of Ministers on 11 September 1995 at the 543rd meeting of the Ministers' Deputies)

the establishment of industrial standards and liability for system quality. In the early years of ICT development, there was more focus on usability. With the development of ICT, a standard for higher quality should be adopted to ensure security.

(2) Promoting security awareness

Cybercrime is merely a serious breach of cybersecurity, which is not ensured because information systems have low controllability. Online users should accept suitable education and training to acquire higher security consciousness. Users are direct interest groups in cybersecurity. Social mechanisms relying on cyber police are simply not enough to maintain cybersecurity. Therefore, it is important for users to raise their law-abiding consciousness, grasp technology to prevent abuses, and enhance their ability of self-protection. To a certain extent, the frequent happening of cybercrime results either from lack of a law-abiding conscience or from the lack of a self-protective consciousness. To educate users is an urgent affair, which should be emphasized at the international level, as the WSIS (2003) has proposed:

"A global culture of cyber-security needs to be promoted, developed and implemented in cooperation with all stakeholders and international expert bodies. These efforts should be supported by increased international cooperation. Within this global culture of cyber-security, it is important to enhance security and to ensure the protection of data and privacy, while enhancing access and trade." (Section B5, paragraph 35)

Some economists may argue that it is prohibitively costly to educate everyone by a specific institution in a specific opportunity at the same time. However, we cannot ignore opportunities for the effective spreading

cybersecurity knowledge to any size of audience. The bottom line for preventive measures the users take is to avoid being victimized.

(3) Raising law-abiding consciousness

Education for the development of a law-abiding conscience follows a tradition of earlier generations, such as Cesare Beccaria.[276] However, law and order in cyberspace has no precedent to follow. It remains disputable as to whether cyberspace constitutes the natural expansion of traditional society. Consequently, it is still arguable whether traditional laws and regulations should be applied to cyber activities, or whether traditional authorities should extend their grasp over a new space. The netizens who migrate to this lawless space behave unconstrainedly. Under cyber sub-culture, hackers defend themselves by their own codes and ethics, refuse to acknowledge the validity of state power, and ignore state jurisdiction over information systems. The assumptions of an anarchic state without regulation or of an autonomic entity with self-regulation are prevalent among technological supremacists. Knowledge and skills make them technical elites on the one hand, ignorance of law and order makes them law-breakers on the other hand. However, in history, talent, knowledge and skills have never become the excuse for crime. Therefore, education is necessary to raise the netizens' law-abiding consciousness in cyberspace just as in society. This law-abiding consciousness falls mostly into the sphere of ethics as well. The "need for ethical management" and "implementing a code" (Bequai 1983, pp. 76-80) has long been recognized. Education in this aspect is a long-term and extensive task for many sectors.

(4) Developing security technology

[276] Crime and Punishment, Chapter 45, 1764.

Before any scientific discovery and technological invention are made available to the general public, they are controlled in the hands of a few scientists and technicians, regardless of the possible impacts. Nothing about security is preferential. Only when incidents of broad harm to human beings became apparent did the scientific ethics begin to be emphasized in obviously harmful scientific activities. Priority should be given to a swift transition from an emphasis on usable technology to the development of a secure technology. The ICT industry has opportunities of developing security technology and of enhancing users' self-protective ability. Information systems can only be secured through a constantly updated technology, the development of new products, increased self-protection, and the closing of security gaps.

(5) Security training

Many factors erode the security protection of information systems. Lack of security consciousness and security measures is the most usual reason why users cannot secure their system. Users do not have the incentive to adopt security measures unless their systems are compromised. The usual examples of active participation in security training take place when users suffer losses or when administrative decree forces them to accept training. Users who benefit from security training are willing to receive further training. Nevertheless, in practice, security training is not always effective if it is operated as a market solution, because private trainers have the incentive of gaining pecuniarily from exaggerating risks and dangers, and from the effects of their training. Therefore, the training should better be organized by qualified institutions licensed by the public authorities.

(6) Establishing specific institutions

Durkheim's ideas concerning the social division of labour argue for specialized organizations in charge of crime prevention. This is because the establishment of institutions specialized in many different fields tends to fall into the hand of a bureaucracy. Social resources are wasted when many new institutions are established while many old institutions are not disestablished. Cybercrime prevention is different. In fact, many countries have established numerous institutions at different levels and on different scales, being affiliated to or independent of other institutions. Independent institutions, equipped with their expertise and knowledge, would be more effective in reacting against urgent incidents. These institutions may take the form of a contact-point such as the 24/ Network designed by the Convention on Cybercrime. The Convention on Cybercrime has provided that each party should authorize a contact-point available on a twenty-four hour, seven-day-a-week base, to guarantee instant support in investigation and collection of evidence.[277] This provision requires member states to bear a round-the-clock responsibility for "immediate assistance."[278]

(7) Reasonably monitoring online activities

Although there are uncertain factors for maintaining law and order in cyberspace, criminal behaviour should be punished and prevented. The establishment of cyber police and cybercrime reaction forces in many countries meets the demand of security protection. One of the goals of a cyber police and of cybercrime reaction forces is to prevent and monitor harmful online activities, which usually happen within seconds and leaves no trace. The fundamental

[277] Convention on Cybercrime, Article 35 24/7 Network.
[278] ibid.; see also HE 153/2006, General Justifications, 4 Effects of the Proposal.

requirements for cyber police should be profound computing and networking knowledge and anti-hacking skills, as well as the potential to follow new developments of ICT. Because cybercrime can easily cross state borders, rapid reaction and the mutual assistance of cyber police between different countries is vital.[279]

(8) Legislating on cybersecurity

Consensus has not yet been reached on whether cyberspace should be regulated or deregulated. However, our discussion supports feasible and adequate regulation, without which law and order in cyberspace cannot be maintained. At present, the legal provisions on cybersecurity protection are scattered throughout criminal law, civil law, specific acts, regulations and

---

279 More than any other recommendations, advice on policing the Internet would induce the biggest controversy and criticism, from organizations and groups such as the ACLU, ISPA, EFF, etc.

The mission of the American Civil Liberties Union (ACLU) is to preserve freedom of speech, association and assembly, right to equal protection under the law, right to due process, and right to privacy. The Union is concerned about the issues including but not limited to anonymity on the web, Internet free speech, Internet privacy, Internet censorship, surveillance and wiretapping, and workplace privacy, etc. (see ACLU website, at http://www.aclu.org/).

The Internet Service Providers' Association (ISPA) strives for promoting competition, self-regulation and the development of the Internet industry, and concerns about the issues such as political monitoring, etc. (see ISPA website, at http://www.ispa.org.uk).

The Electronic Frontier Foundation (EFF) fights for the right to free speech, as detailed as the right to blog anonymously, the right to keep sources confidential, the right to make fair use of intellectual property, the right to allow reader's comments without fear, the right to protect the servers from government seizure, the right to freely blog about elections, the right to blog about the workplace, and the right to access the media (see EFF website, at http://www.eff.org/br/).

See also other organizations or groups, for example the Internet Free Expression Alliance (IFEA, at http://www.ifea.net/), the Digital Freedom Network (DFN, at http://www.iia.org/dfn/), the Computer Professionals for Social Responsibility (CPSR, at http://cpsr.org/home), the Electronic Privacy Information Centre (EPIC, at http://www.epic.org/), and the Centre for Democracy and Technology (CDT, http://www.cdt.org/cda.html).

decisions. It is necessary to implement a law specializing in cybersecurity protection, during which the lessons and experiences of various countries should be drawn upon to strengthen pertinence, systematism, and operability. The improved effectiveness of regulation and an increased severity in punishment would make it more costly to commit cybercrime, and discourage the potential criminals from taking the risk.

(9) Reinforcing judicial effectiveness

The ICT promotes the effectiveness of all the social activities by making all the participants informed. Cybercrime emerges as a side-product of ICT, which can both strengthen and weaken the effectiveness of the law enforcement based on the traditional social environment. The central problem is that the atmosphere of free cyberspace has an extensive influence. When interception techniques are used in law enforcement, they usually induce disputes from different interest groups. The culture of security should be promoted by the adoption of relevant techniques by the law-enforcement agencies.

(10) Cooperation of the public-private sectors

Cybersecurity is a relative conception and mixed provision is more efficient. Cybersecurity should be primarily maintained by the private sector, assisted by the public sector, represented by law enforcement. Because of conflict of interests and limited capacity, neither public sector nor private sector can undertake the whole task of cybersecurity protection alone. The absence of public-private cooperation has been one of the critical problems in combating cybercrime (Syngress 2002, p. 2), lack of which just leaves loopholes in cybersecurity unfilled and exposes the vulnerabilities of information systems.

International society has recognized the importance of cooperation in this field.[280] Three modes of public-private cooperation should be considered: first, public-private partnership; second, public-supported private activities; and third privately-supported public activities. Previously, cooperation was usually organized by the public sector and participated in by the private sector. The authoritative power and administrative function of the public sector played an important role in inducing a broad participation of individuals and enterprises, providing some kinds of education, training, rules, and coordination. The growing interests and forces of the private sector require a strengthened role in providing cybersecurity independently, or interdependently with the public sector.

(11) International cooperation

The international highway, railway and airway are limited to territory. The material existence of an information superhighway, however, only appears in sovereignties in the forms of cables and computers. The contents and activities of information systems are intangible, crossing locations distributed possibly anywhere along the "information superhighway." The discussions in the previous chapters have offered abundant revelation that in the current greatly interconnected society, combating cybercrime necessitates global cooperative endeavours, which is required in cybersecurity protection at various levels, including raising international and national levels of security consciousness, harmonizing substantive legislations, filtering and intercepting trans-border information traffic, furthering the exchange of detained judicial information,

---

280 Council of Europe, Preamble, Convention on Cybercrime, Budapest, 23 November 2001.

mutual assistance in criminal investigation, extradition of criminals, and other necessary fields. McConnell International has (2000, p. 8) proposed a "model approach" to cover both international cooperation and private-public partnership to eradicate the legal vacuum. The "common criminal policy" as the Convention on Cybercrime furnishes can be seen as equivalent.[281] A consistent framework of legal policy constitutes the foundation of any international cooperation. In international cooperation, this means the necessary *coordinated* national police actions in search and seizure of stored data, real time collection of traffic data, interception of content data, and so on as provided in the Convention on Cybercrime (Articles 19-21).

The present world powers remain in the status intolerant of differences between communities, countries, and cultures. History repeatedly proved that ours is a world without awaiting and communication before state violence and wars come into being. The failure of broader consensus and broader accommodation of the current international forum reminds the mutual proximity through international, intercultural and interrelated dialogue. The natural logic behind this world is that in a violent world, terrorism has been the excuse of endless wars (against the terrorists) and in information society, cyber terrorism will be the excuse of future wars (against the cyber terrorists). It seems that international cooperation in an equal and a tolerant platform is more than ever required. In the sense of money laundering, developed states, particularly those with a developed banking system, are legally doing far more than a poor country listed as the core of world concern can implicitly or explicitly do.[282]

[281] ibid.

[282] For example, Myanmar is currently the only country listed by Financial Action Task

However, international pressure is more than ever put on the poor country rather than its developed counterparts. Therefore, future international cooperation should be carried out in a more balanced way, an approach that should run through all efforts for combating cybercrime.

(12) Reinforcing the deterrence of punishment

Penal measures are the final remedy for cybersecurity breaches. If criminals are left unpunished, they will have a greater incentive to repeat their activities and gaining even more pecuniary profit from them. Legal history has not witnessed any substitutive measures for punishments, even though the types of punishments change over time.[283] The previous practice proves that deterrence of punishment has been greatly influenced by obstacles to law enforcement. The economic viewpoint on crime and justice argues that low probability of detection and inappropriate severity of punishment would minimize the overall deterrence (Becker 1968). In order to improve the deterrent effect of punishment, both investigation and conviction should be strengthened through a series of techniques and actions. Both national and international legal instruments have been constantly making such efforts.[284] Nevertheless, there are

---

Force on Money Laundering (TAFT) as Non-Cooperative Countries and Territories (NCCT) in the field of anti-money laundering. See TAFT web site, 23 June 2006. Retrieved 15 February 2016, from http://www.fatf-gafi.org/document/4/0,2340,en_32250379_32236992_33916420_1_1_1_1,00.html

[283] The most ancient punishments were characterised by physically exterminating or torturing criminals, including capital and corporal punishments, even though fine and imprisonment were similarly old. The later punishments became less bloody and less cruel, primarily depriving freedom and dignity. The latest tendency is that punishments indirectly related to the criminals' life, health and freedom are broadly adopted, including fine, disqualification, community service, and probation.

[284] For example, the Council of Europe Convention on Cybercrime, European Union Framework Decision on Attacks against Information System, HE 153/2006 of Finland, and so forth. The mechanisms include the acquiring and fixing of digital evidence, duty of witness, international information exchange, etc.

also factors hindering the extreme efforts to reduce the crime-rate simply by increasing investment for improving law enforcement. It would be prohibitively expensive to produce a few effects on crime rate reduction. Therefore, no better alternative is open than that of giving comprehensive consideration to the process of law enforcement in a detailed social context.

(13) Establishing a victim compensation mechanism

Cybercrime represents a way of transferring information, wealth, competitive power, and psychological satisfaction from victims to perpetrators. Most victims are usually those people with low risk-awareness and a low security level. Furthermore, the victims of cybercrime are generally reluctant to report crimes. They worry that public authorities cannot remedy past damage but can cause further losses by weakening public reputation and inducing future attacks. Victim compensation mechanisms increase the incentives of victims to report crimes and provide evidence, with the help of which they can recover part of losses. Because compensation imposes an extra financial burden on the perpetrators, it also creates incentives to discourage the potential criminals from compromising information systems. Ideally, the dual incentives thus created will decrease the number of cybercrimes.

(14) Eliminating negative incentives in cybersecurity protection

Cybersecurity involves many different interest groups who benefit from different activities. System developers attempt to reduce costs for improving the security of software. Computer users attempt to reduce their investment on security measures. Security service providers have the incentive to exaggerate the risks, dangers, number and losses of insecurity incidents. The mass media also have the incentive to attract more readers, audience, advertisers, and

marketers. Even the police and professors have the possibility of benefiting from increased expenses on research and development. On the other hand, some individuals and institutions have an incentive to underestimate the genuine threat of cybercrime. Countermeasures must be taken to eliminate these incentives that distort truths and exploit these distorted truths of cybersecurity.

(15) Drawing out lessons from the experiences of traditional crime-prevention practice

Although cybercrime has many characteristics different from traditional offences, it is a natural development of criminal phenomena, playing an interference opportunities brought about by information systems. The past lessons in failed efforts and experiences in successful endeavours have an organic relationship with current and future-policy design. In fields such as the deterrence of juvenile delinquency, international trafficking of human beings, drug control, and prevention of violence, the existing criminal-justice system proves constructive. The cybercrime scene is less violent, but there are still elements that can be addressed by ordinary methods, such as raising a law-abiding consciousness, by constructing an online community, and by the establishment of an information security culture.

With all these measures, our intent is to increase the effectiveness of deterrence and to reduce the benefits of cybercrime, ensuring that the existing and potential perpetrators will be less satisfied. Mathematical methodology usually reduces crime prevention to some numerical indicators unreliably. Schweinhart, Barnes, and Weikart (1993) found that each dollar spent on crime prevention would ultimately save seven dollars (cited in Levinson 2002, p. 696). We could hardly anticipate that this kind of precise calculation of the preventive

effect would ensure a constructive method for providing generalized policy recommendations. Mathematical or statistical methods are typically overused and misleading in contemporary social sciences. Although it is unreasonable to suppose that spending more money would reduce the losses caused by cybercrimes, or simply decrease the number of cybercrimes, measures against cybercrime will definitely involve more investment. Besides pecuniary involvement, many other aspects of social forces should in addition be taken into account to enforce the counter-cybercrime efforts. Thus, both money and staff will have to be dumped into this endless circulation of crime and anti-crime, or anti-social behaviour and anti-anti-social endeavour. While criminal phenomena are a comprehensive erodent to the economic society, the distinct measures undertaken against them must be integrated in order to deter intrigue against the prosecution of offences. In this way, the abandoned hope of society may be restored to it. Great challenges necessitate powerful commitment.

The long-term and sustainable actions are to be aimed at the reduction of factors benefiting the occurrence of cybercrime and the augmentation of factors benefiting the maintenance of cybersecurity. This necessitates a social-control model through a relatively open and decentralized legal system, overcoming the closed and centralized faults inherited from the tradition of legalism. Furthermore, law is reduced by information systems into a minor method of social control, from the starting-point where it was once the dominant method, or at least a parallel method to other social-control methods. There is hardly a legal superhighway that leads to the normalization of the information superhighway.

BIBLIOGRAPHY

Adamson, J. E. 2006. *Law for Business and Personal Use*, Mason, Ohio: Thomson South-Western.

Allan, R. A. 2001. *A History of the Personal Computer: The People and the Technology*, London, Ontario: Allan Publishing.

Allen, J. 2001. CERT System and Network Security Practices, in *Proceedings of Fifth National Colloquium for Information Systems Security Education*, George Mason University, Fairfax, Virginia, 22-24 May. Retrieved 15 February 2016, from http://www.theebusinesssite.com/PPT/SecureWebsites-769468/769498_Reading_Class8-CERT_Network_Hardening.pdf

Alvesalo, A., and Laitinen, A. 1994. *Perspectives on Economic Crime*, Turku: Painosalama.

American Society for Industrial Security (ASIS). 2004. Cybercrime-Fighting Tools Still Lacking, *Security Management*, number 40.

Anderson, R. 2001. Why Information Security Is Hard--an Economic Perspective, in *Proceedings of the 17th Annual Computer Security Applications Conference*, Washington, DC: IEEE Computer Society. Retrieved 15 February 2016, from http://www.acsac.org/2001/papers/110.pdf

APEC. 2001. *Leaders Statement on Counter-Terrorism*, APEC Economic

Leaders' Meeting, Shanghai, 21 October.

APEC. 2002. *Recommendation by the APEC Telecommunications and Information Working Group (TEL) to APEC Senior Officials (SOM) for an APEC Cybersecurity Strategy*, 2002/CSOM/052, Concluding Senior Officials Meeting, Los Cabos, B. C. S., Mexico, 21-22 October.

APEC. 2003. *Conference Report: Cybercrime Legislation and Enforcement Capacity Building Project*, 21-25 July, Bangkok, Thailand.

Archick, K. 2004. *Cybercrime: The Council of Europe Convention, CRS Report for Congress*, Order Code RS21208, Congress Research Service, 22 July.

Aromaa, K., and Laitinen, A. 1994. *Juvenile Delinquency and Business Security*, Helsinki: Painatuskeskus.

Association for Computing Machinery. 1997. *Professional Knowledge Programme*. New York, NY: Association for Computing Machineray.

August, R. 2002. International Cyber-Jurisdiction: A Comparative Analysis, *American Business Law Journal*, volume 39, number 4, pp. 531-573.

Australian Computer Emergency Response Team. 2002. *2002 Australian Computer Crime and Security Survey*.

Australian Computer Emergency Response Team. 2003. *2003 Australian Computer Crime and Security Survey*.

Australian Computer Emergency Response Team. 2004. *2004 Australian Computer Crime and Security Survey*.

Australian Computer Emergency Response Team. 2005. *2005 Australian Computer Crime and Security Survey*.

Australian Computer Emergency Response Team. 2006. *2006 Australian Computer Crime and Security Survey*.

Australian Computer Emergency Response Team. 2012. *2012 Australian Computer Crime and Security Survey*.

Australian Computer Emergency Response Team. 2013. *2013 Australian Computer Crime and Security Survey*.

Australian Computer Emergency Response Team. 2015. *2015 Australian Computer Crime and Security Survey.*

Banks, M. A. 1997. *Web Psychos, Stalkers, and Pranksters: How to Protect Yourself Online*, Arizona (USA), The Coriolis Group.

Becker, G. S. 1968. Crime and Punishment: An Economic Approach, *Journal of Political Economy*, volume 76, pp. 169-217.

Becker, J. January 1981. Who Are the Computer Criminals? *Security Management*, pp. 18-20.

Behar, R. 1997. Who's Reading Your E-mail? *Fortune*, number 66, pp. 57-70.

Bell, D. 1974. *The Coming of the Post-Industrial Society*, London: Heinemann.

Bequai, A. 1978. *Computer Crime*, Lexington, Massachusetts, Toronto: Lexington Books.

Bequai, A. 1979a. *White-Collar Crime: A 20th Century Crisis*, Lexington, Massachusetts: Lexington Books.

Bequai, A. 1979b. *Organized Crime*, Lexington, Massachusetts, Toronto: Lexington Books.

Bequai, A. 1983. *How to Prevent Computer Crime: A Guide for Managers*. New York, Chicago, Brisbane, Toronto, Singapore: John Wiley and Sons.

Berg, T. 2000. WWW.Wildwest.gov: The Impact of the Internet on State Power to Enforce the Law, *Brigham Young University Law Review*, volume 2000, number 4, pp. 1305-1362.

Berman, P. S. 2002. Globalization of Jurisdiction, *University of Pennsylvania Law Review*, volume 151, number 2, pp. 311-545.

Biegel, S. 25 January 1996. The Emerging and Specialized Law of the Digital Revolution, *Los Angeles Daily Journal*.

BloomBecker, J. 3 August 1981. Employee Computer Abuse –What to Do? *The Los Angeles Daily Journal*, pp. 16-17.

Bossard, A. 1997. International Crime (Chinese translation), *Commercial Press*.

Bourne, C. P. and Hahn, T. B. 2004. *A History of Online Information Services, 1963-1976*, Massachusetts Institute of Technology Press.

Bourne, R. 2002. Commonwealth Law Ministers' Meeting: Policy Brief, Commonwealth Policy Studies Unit, Institute of Commonwealth Studies, University of London.

Branscomb, R. 1990. Computer Program and Computer Rogues: Tailoring the Punishment to Fit the Crime, *Rutgers Computer and Technology Law Journal,* volume 16, pp. 1-61.

Brenner, S. W. 2001. Cybercrime Investigation and Prosecution: the Role of Penal and Procedural Law. Retrieved 15 February 2016, from http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN003073.pdf

Brenner, S. W. 2002. Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships, *North Carolina Journal of Law and Technology*, volume 4, number 1.

Brenner, S. W. and Koops, B-J. 2004. Approaches to Cybercrime Jurisdiction, *Journal of High Technology and Law*, volume 4, number 1.

Bush, G. W. 17 November 2003. Message to the Senate of the United States

on the Cybercrime Convention, Office of the Press Secretary.

Bynum, T. 2001. Computer Ethics: Basic Concepts and Historical Overview, in *Stanford Encyclopaedia of Philosophy*. Retrieved 15 February 2016, from http://plato.stanford.edu/entries/ethics-computer/

Carter, D. L. 1995. Computer Crime Categories, *Law Enforcement Bulletin*, U. S. Department of Justice: Federal Bureau of Investigation, volume 64, number 7, pp. 21-26.

Casey, E. 2000. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. London: Academic Press.

Castells, M. 1985. High Technology, Economic Restructuring, and the Urban-Regional Process in the United States, in Manual Castells. (ed.). *High Technology, Space, and Society, Urban Affairs Annual Reviews*, volume 28, Beverly Hills, London, New Delhi: Sage Publications, 1985, pp. 11-40.

CCIPS. 2006. Computer Intrusion Cases. Retrieved 15 February 2016, from http://www.usdoj.gov/criminal/cybercrime/cccases.html

Center for Strategic and International Studies (CSIS). 2015. Net Losses: Estimating the Global Cost of Cybercrime. Washington, DC: The Center for Strategic and International Studies.

Chen, C. D. 1990. Computer Crime and the Computer Fraud and Abuse Act of 1986, *Computer Law Journal*, volume 10, number 1, pp. 71-86.

China National Networks Information Centre. 2006. *Statistical Survey Report on the Internet Development in China (2006)*, Beijing.

Clark, F. and Diliberto, K. 1996. *Investigating Computer Crime*, Boca Raton, Florida: CRC Press LLC, 1996.

Clarke, A. C. 1997. *3001: The Final Odyssey*, Hammersmith, London:

Voyager.

Clarke, A. C.1984. *1984: Spring*, London: Granada Publishing.

Cohen, F. 1984. Computer Viruses-Theory and Experiments, *IFIP TC 11 Conference*, Toronto. Retrieved 15 February 2016, from http://www.all.net/books/virus/index.html

Cohen, L. E., and Felson, M. 1979. Social Change and Crime Rate: A Routine Activity Approach, *American Sociological Review*, vol. 44, pp. 588-608.

Coleman, J. S. 1990. *Foundations of Social Theory*. Cambridge, Massachusetts, and London, England: The Belknap Press of Harvard University Press.

Collin, B. C. 1999. The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge, *11th Annual International Symposium Criminal Justice Issues*. Retrieved 15 February 2016, from http://www.crime-research.org/library/Cyberter.htm

Commission of the European Communities. 2000. *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime,* COM (2000) 890 final.

Commission of the European Communities. 2002. *Proposal for a Council Framework Decision on Attacks against Information Systems*, COM (2002) 173 final.

Committee to Study the Impact of Info, National Research Council Commission, 1994. *Information Technology in the Service Society*, Washington, D. C.: National Academy Press.

Computer Science and Telecommunications Board, National Research Council, 2002. *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*, Washington, D.C.: National Academy Press.

Conly, C. H. 1991. *Organizing for Computer Crime Investigation and Prosecution*, Darby, PA: Diane Publishing.

Cook, D. 1997. *Poverty, Crime and Punishment*, London: CPAG.

Cooley, C. H. 1983. *Social Organization*, New Brunswick, New Jersey: Transaction Publishers.

Cooter, R. and Ulen, T. Law and Economis, fourth edition, Addison Wesley, 2003.

Cornwall, Hugo. 1987. *Datatheft: Computer Fraud, Industrial Espionage and Information Crime*, London: Heinemann.

Cortada, J. W. 2002. *Making the Information Society: Experiences, Consequences, and Possibilities*, Englewood Cliffs, New Jersey: Prentice Hall PTR.

CSI. 2000. CSI/FBI 2000 Computer Crime and Security Survey.

CSI. 2001. CSI/FBI 2001 Computer Crime and Security Survey.

CSI. 2002. CSI/FBI 2002 Computer Crime and Security Survey.

CSI. 2003. CSI/FBI 2003 Computer Crime and Security Survey.

CSI. 2004. CSI/FBI 2004 Computer Crime and Security Survey.

CSI. 2005. CSI/FBI 2005 Computer Crime and Security Survey.

CSI. 2006. CSI/FBI 2006 Computer Crime and Security Survey.

CSI. 2008. CSI/FBI 2008 Computer Crime and Security Survey.

CSI. 2011. CSI/FBI 2011 Computer Crime and Security Survey.

Cybercrime Convention Committee (T-CY). 2015. Criminal Justice Access to Data in the Cloud: Challenges. Retrieved 15 Februrary 2016, from http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTM Content?documentId=0900001680304b59.

Daintith, J. (eds.). 2004. *Oxford Dictionary of Computing*, fifth edition, Oxford:

Oxford University Press.

Daler, T., Gulbrandsen, R., Melgrd, B. and Sjølstad, T. 1989. *Security of Information and Data*, Chichester: Ellis Horwood.

Royall, D. and Hughes, M. 1990. *Computerization in Business*, Long Acre, London: Pitman Publishing.

Davidson, A. 14 April 2003. Decentralization, Disease and Terrorism. Retrieved 15 February 2016, from http://www.eclicktick.com/decentralization__disease_and_terrorism__.htm

Debose, B. 29 January 2004. Kerry Says Threat of Terrorism Is Exaggerated, *The Washington Times*.

Dibbell, J. 1993. A Rape in Cyberspace, *Village Voice*, volume XXXVIII, number 51, pp. 36-42.

Didsbury, H. F. (ed.). 1982. *Communications and the Future,* World Future Society.

Dierks, M. P. Computer Network Abuse, *Harvard Journal of Law and Technology*, volume 6, 1993, pp. 307-342.

Digital Equipment Corporation (DEC). 1963. *Programmed Data Processor-1 Handbook*, Maynard, Massachusetts.

Dnes, A. W. 2000. The Economics of Crime, in N. G. Fielding, A. Clarke and R. Witt. (eds.). *The Economic Dimensions of Crime*, London: Palgrave, 2000, pp. 70-81.

Dong, B. 15 October 2003. Eighty Percent of Net Café Consumers are Youths, *China Youth Newspaper*.

Dong, S. and Li, X. 2015. ЗАЩИТА ЛИЧНОЙ

ПОЛЬЗОВАТЕЛЬСКОЙ ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ: ДИЛЕММЫ ПРАВООХРАНИТЕЛЬНОЙ ПРАКТИКИ КИТАЯ (Dilemmas in Defending Privacy in Social Networking Services: With Special Regard to Practice of China). *Legal Science and Law Enforcement Practice*, 34 (4), pp. 170−179.

Drummond, N., and McClendon, D. J. 2001. Cybercrime- Alternative Models for Dealing with Unauthorized Use and Abuse of Computer Networks. Retrieved 15 February 2016, from http://gsulaw.gsu.edu/lawand/papers/su01/drummond_mcclendon/

Duckett, L. 22 March 1996. Special Assistant to DC Police Chief; President, Black Police Caucus, *The Washington Post*.

Dunlop, C and Kling, R. 1991. Introduction to Security and Reliability, in C. Dunlop and R. Kling (eds.) *Computerization and Controversy: Value Conflicts and Social Choices*, San Diego: Academic Press, 1991, pp. 524-532.

Dunlop, C. and Kling, R. (eds.). 1991. *Computerization and Controversy: Value Conflicts and Social Choices*, San Diego: Academic Press.

Dvorak, J. C., and Pirillo, C. 2004. *Online!* Pearson Education.

Elliot, M. A. and Merrill, F. E. 1961. *Social Disorganization*, fourth edition, New York, Evanston, and London: Happer and Row Publishers.

E-Security Task Group. 2003. *E-Security Task Group, Cybercrime Legislation and Enforcement Capacity Building Project*, 21-25 July, Bangkok, Thailand.

Fager, C. 9 December 2004. The 419 Fraud, *Christianity Today*, volume 46, number 13, p. 20.

Feldman, P. 1993. *The Psychology of Crime*, New York, NY: Cambridge University Press.

Felson, M. 2002. *Crime and Everyday Life*, third edition, Thousand Oaks, California: SAGE Publications.

Fetherolf S. 1982. Telecommunications and the Future, in H. F. Didsbury (ed.) *Communications and the Future*, World Future Society, pp. 211-222.

Fidler, M. 2015. The African Union Cybersecurity Convention: A Missed Human Rights Opportunity. Retrieved 15 February 2016, from http://blogs.cfr.org/cyber/2015/06/22/the-african-union-cybersecurity-convention-a-missed-human-rights-opportunity/.

Fielding, N. G., Clarke, A. and Witt, E. 2000. *The Economic Dimensions of Crime*, London: Palgrave.

Fields, G. 6 April 2004. Cyberexperts and Engineers Wanted by FBI, *Wall Street Journal*, B1.

Findlay, M. 1999. *The Globalization of Crime: Understanding Transitional Relationships in Context*, Cambridge: Cambridge University Press.

Fisk, M. 2002. Causes and Remedies for Social Acceptance of Network Insecurity, *Workshop on Economics and Internet Security 2002*.

Fooner, M. 1989. *Interpol: Issues in World Crime and International Criminal Justice*, New York and London: Plenum Press.

Forester, T. 1990. Software Theft and the Problem of Intellectual Property Rights, *Computer and Society*, volume 20, number 1, pp. 2-11.

Forester, T. and Morrison, P. 1994. *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing*, second ed., London: MIT Press.

Franklin, M. 2006. Suggested Best Practice for Pursuing Development and Poverty Reduction through National ICT Strategies, *Journal of Eastern Caribbean Studies*, vol. 31, no. 4, December 2006, pp. 85-104.

Freeh, L. J. 28 March 2000. *Statement for the Record of Louis J. Freeh, Director FBI on Cybercrime Before the Senate Committee (Judiciary Subcommittee for the Technology, Terrorism, and Government Information),* Washington, D.C. Retrieved 15 February 2016, from http://www.cybercrime.gov/freeh328.htm

Friedrichs, D. 1996. Trusted Criminals-White-Collar Crime in Contemporary Society. Belmont, California: Wadsworth Publishing Company.

F-Secure. 2005. F-Secure Expands Asian Business and Launches First Major Internet Service Provider Relationship. Retrieved 15 February 2016, from http://www.f-secure.com/news/items/news_2005092800.shtml.

Fulford, R. 22 December 1993. As a Rule, Canadians Love to Regulate, *The Globe and Mail*, C1.

G7. 17 June 1995. Chairman's Statement, *Halifax G7 Summit.*

Gao, Z. 2006. Hacker Tried for Theft of 3.7 Million from Beijing Mobile. Retrieved 15 February 2016, from http://www.chinacourt.org/public/detail.php?id=196319

Garrison, L. and Grand, M. (eds.). 2001. Cyberterrorism: An Evolving Concept, *National Infrastructure Protection Centre (NIPC) Highlights*, number 6-01, 15 June 2001, p. 2. Retrieved 15 February 2016, from http://www.iwar.org.uk/infocon/nipc-highlights/2001/highlight-01-06.pdf

Gates, B. 1995. *The Road Ahead,* New York: Viking.

Geis, G. and Goff, C. 1983. Introduction, in Edwin H. Sutherland, *White Collar* Crime (the uncut version), with an introduction by Gilbert Geis and Colin Goff, New Haven and London: Yale University Press, 1983.

Gelbstein, E., and Kamal, A. 2002. *Information Insecurity: A Survival Guide to the Uncharted Territories of Cyber-threats and Cyber-security*, the United Nations Information and Communications Technology Task Force and the United Nations Institute for Training and Research.

Geng, F. 27 February 2003. Zhengzhou Internet Users Abducted and Raped a Young Girl, *Pingliang Daily*.

Gibson, W. 1984. *Neuromancer*, New York: Ace Books.

Goldsmith, J. 2005. The Internet and the Legitimacy of Remote Cross-Border Searches, *Chicago Public Law and Legal Theory Working Paper*, number 16, The Law School, The University of Chicago.

Goodman, M. D. 1997. Why the Police Don't Care About Computer Crime, *Harvard Journal of Law and Technology*, volume 10, number 3, pp. 465-494.

Gore, A. 21 March 2004. *Speech to the International Telecommunications Development Conference*, Buenos Aires.

Grabosky, P. 2000. Cyber Crime and Information Warfare, The Transnational Crime Conference convened by the Australian Institute of Criminology in association with the Australian Federal Police and Australian Customs Service and held in Canberra, 9-10 March. Retrieved 15 February 2016, from http://www.aic.gov.au/conferences/transnational/grabosky.pdf

Grabosky, P. 2004. Global Dimension of Cybercrime, *Global Crime*, vol. 6, no. 1, pp. 146-157.

Grabosky, P., Smith, R. G. and Dempsey, G.. 2001. *Electronic Theft: Unlawful Acquisition in Cyberspace*, Cambridge: The Press Syndicate of the University of Cambridge, 2001.

Grauer, M. 2001. Information Technology, Information and Knowledge, in

N. J. Smelser and P. Bates (eds.). *International Encyclopaedia of the Social and Behavioral Sciences*, New York, N.Y.: Elsevier, volume 11, 2001, pp. 7475-7476.

Gray, C. M. 1979. The Costs of Crime: Review and Overview, in C. M. Gray. (ed.). *The Costs of Crime*, Beverly Hills, CA: SAGE Publications, pp. 13-32.

Greenberg, M. S. and Ruback, R. B. 1985. A Model of Crime Victim Decision Making, *Victimology: An International Journal*, volume 10, pp. 600-616.

Griffin, N. 2001. *The Selected Letters of Bertrand Russell: The Public Years, 1914-1970*, London: Routledge.

Grimm, D. 2005. "Security Breach" Leaks NIH Grant Applications Onto Web, *Science*, 28 October, vol. 310. no. 5748, p. 598, DOI: 10.1126/science.310.5748.598.

Group of Eight Justice Ministers. 1998. The Joint Release, *Virtual Meeting on Organized Crime and Terrorist Funding*.

Group of Eight. 1997. Communiqué, Denver, 22 June 1997, *Denver Summit of the Eight*, 20-22 June.

Group of Eight. 2000. *Conference on Dialogue Between the Public Authorities and Private Sector on Security and Trust in Cyberspace Final Press Release* Paris, France, 15-17 May.

Guo, Q. and Wang, Y. 29 July 2003. Cruel Woman Invited Net Friend to Kill Her Husband, Police Found Murder Evidence from Internet, *Great River Newspaper*.

Hafner, K., and Lyon, M. 1998. *When Wizards Stay up Late: The Origins of the Internet*, New York: Simon and Schuster, pp. 10-14.

Hagerty, L. C. 2000. *The Spirit of the Internet*, Tampa, Florida: Matrix Masters.

Hale, C. 2002. Cybercrime: Facts and Figures Concerning the Global Dilemma, *Crime and Justice International*, volume 18, number 65.

Hamilton, D. 1973. *Technology, Man and the Environment*, London: Faber and Faber.

Harvey, F. 3 December 2003. Online Crime Set to Rise: Cyberspace: The Fight against Hackers Is a Big Burden, *Financial Times*.

Hatcher, M. and co-workers. 1999. Computer Crimes, *American Criminal Law Review*, volume 36.

Helmkamp, J., Ball, R., and Townsend, K. 1996. Proceedings of the Academic Workshop: "Definitional Dilemma: Can and Should There Be a Universal Definition of White-collar crime?" Morgantown, West Virginia: National White-collar crime Centre.

Himanen, P. 2001. *The Hacker Ethic and the Spirit of Information Age*, Great Britain, Secker and Warburg.

Hoo, J. S. 2000. How Much is Enough? A Risk Management Approach to Computer Security, *Centre for International Security and Cooperation Working Paper*. Retrieved 15 February 2016, from http://iis-db.stanford.edu/pubs/11900/soohoo.pdf

Howerton, P. W. 1985. *Computer Crime: A Tutorial*, ACM.

Howitt, D. 2002. *Forensic and Criminal Psychology*, Essex, England: Pearson.

Icove, D., and co-workers. 1995. *Computer Crime: A Crimefighter's Handbook*, O'Reilly and Associates.

International Monetary Fund (IMF). 2002. *Global Financial Stability Report, A Quarterly on Market Developments and Issues*, International Monetary Fund.

Internetworldstats.com. 2007. Internet Usage Statistics-The Big Picture. Retrieved 27 July 2007, from http://www.internetworldstats.com/stats.htm.

Internetworldstats.com. 2015. Internet Usage Statistics-The Big Picture. Retrieved 15 February 2016, from http://www.internetworldstats.com/stats.htm.

Interpol. 2014a. Criminal Network Involved in Payment Card Fraud Dismantled with Interpol Support. Retrieved 15 February 2016, from http://www.interpol.int/News-and-media/News/2014/N2014-074

Interpol. 2014b. Global Action against Online Fraud in the Airline Sector Nets 118 Arrests. Retrieved 15 February 2016, from http://www.interpol.int/News-and-media/News/2014/N2014-228.

Interpol. 2015a. Illegal online Gambling in Asia Targeted in Interpol Operation. Retrieved 15 February 2016, from http://www.interpol.int/News-and-media/News/2015/N2015-109.

Interpol. 2015b. More than 130 Detained in Global Action Tackling Airline Ticket Fraud. Retrieved 15 February 2016, from http://www.interpol.int/News-and-media/News/2015/N2015-181.

Interpol. 2015c. More than 500 Arrested in Interpol Operation Targeting Phone and Email Scams. Retrieved 15 February 2016, from http://www.interpol.int/News-and-media/News/2015/N2015-223.

Jew, B. 1999. Cyberjurisdiction? Emerging Issues and Conflicts of Law When Overseas Courts Challenge Your Web. Retrieved 15 February 2016, from http://www.gtlaw.com.au/t/publications/default.jsp?pubid=76

Jiang, H. and Yu, Z. 1997. Concerning Offence of Creating and Spreading Destructive Computer Program, *Jurists*, number 5, pp. 18-27.

Jiang, P. 2000. *A Study on Computer Crime*, Commercial Printing Company, pp. 151-152.

Johnson, D. R. and Post, D. 1996. Law and Borders—The Rise of Law in Cyberspace, *Stanford Law Review*, volume 48, number 5, pp. 1367-1402.

Johnson, T. A. 2006. *Forensic Computer Crime Investigation*, Boca Raton, Florida: Taylor and Francis Group.

Jones, C. W. 2005. Council of Europe Convention on Cybercrime: Themes and Critiques, *Workshop on the International Dimensions of Cyber Security, hosted by the Georgia Institute of Technology and Carnegie Mellon University*, 6-7 April.

Jones, S. 2003. *Encyclopedia of New Media: an Essential Reference to Communication and Technology*, Sage Publications.

Jordan, T. and Taylor, P. A. 1998. Sociology of Hackers, *Sociological Review*, volume 46 number 4, pp. 757-81.

Kabay, M. E. 2001. Studies and Surveys of Computer Crime. Retrieved 15 February 2016, from http://www2.norwich.edu/mkabay/methodology/crime_studies.htm

Kaczynski, T. 1995. *The Unabomber's Manifesto: Industrial Society and Its Future*, Jolly Roger. Retrieved 15 February 2016, from http://en.wikisource.org/wiki/Industrial_Society_and_Its_Future

Katyal, N. K. 2001. Criminal Law in Cyberspace, *University of Pennsylvania Law Review*, volume 149, pp. 1003-1114.

Kavanagh, P. 2004. *Open Source Software: Implementation and Management*, Oxford: Elsevier Digital Press.

Kehoe, B. P. 1993. *Zen and the Art of the Internet*, Englewood Cliffs, New Jersey: PTR Prentice Hall.

Kelly, J. X. 2002. Cybercrime - High Tech Crime, JISC Legal Information Service - University of Strathclyde. Retrieved 15 February 2016, from http://www.jisc.ac.uk/legal/index.cfm?name=lis_cybercrime

Kenneally, E. 2001. Inside: Sysadmine- Stepping on the Digital Scale, *";Login: The Magazine of Usenix and Sage"*, volume 26, number 8, pp. 61-77.

Kiger, M., Arkin, O. and Stutzman, J. 2004. *Profiling. In The Honeynet Project Know Your Enemy: Learning about Security Threats*, Addison Wesley.

Kingdon, J. 1994. Shooting the Messenger: The Liability of Internet Service Providers for Prohibited Expression. Retrieved 15 February 2016, from http://www.catalaw.com/logic/docs/jk-isps.htm

Kling, B. 1980. Computer Abuse and Computer Crime as Organizational Activities, *Computer/Law Journal*, vol. II, no. 2, pp. 12-24.

Koch, L. Z. 10 July 2000. Open Sources Preventing Cybercrime, *Inter@ctive Week*.

Kollock, P. and Smith, M. 1999. Communities in Cyberspace, in: M. Smith and P. Kollock (eds), *Communities in Cyberspace*, London: Routledge, pp. 3-28.

Kovacich, G. and Boni, W. C. 1999. *High Technology Crime Investigator's Handbook: Working in the Global Information Environment*, Burlington, Massachusetts: Butterworth-Heinemann.

Kremen, S. H. 1998. Apprehending the Computer Hacker: The Collection and Use of Evidence, *Computer Forensics Online*. Retrieved 15 February 2016, from http://www.shk-dplc.com/cfo/articles/hack.htm

Kuck, D. J. 1978. *The Structure of Computers and Computations*, volume 1. New York, Santa Barbara, Chichester, Brisbane, Toronto: John Wiley and Sons.

Lee, M. and co-workers. 1999. Electronic Commerce, Hackers, and the

Search for Legitimacy: A Regulatory Proposal, *Berkeley Technological Law Journal*, volume 14, number 2, pp. 839-885.

Lehtonen, A. 2000a. Legal *Liability of Damages Caused by Computer Virus*, Department of Economic law, Vaasa: University of Vaasa. Retrieved 15 February 2016, from http://lipas.uwasa.fi/ktt/talousoikeus/it/legalliability.html.

Lehtonen, A. 2000b. *Straffrättslig Jurisdiktion över Internet-brott* (Criminal Jurisdiction over Internet Crime), Department of Economic law, Vaasa: University of Vaasa. Retrieved 15 February 2016, from http://lipas.uwasa.fi/ktt/talousoikeus/it/i-brott/ibrott_toc_swe.htm.

Leiwo, J. 1995. *Deterrence of Computer Network Crime*, Oulu: University of Oulu.

Lenk, K. 1997. *The Challenge of Cyberspatial Forms of Human Interaction to Territorial Governance and Policing, The Governance of Cyberspace*, Routledge, New York, 126-135.

Lessig, L. 1996. Zones in Cyberspace, *Stanford Law Review*, volume 48, number 5, pp. 1403-1411.

Levinson, D. (ed.). 2002. *Encyclopedia of Crime and Punishment*, Newbury Park, CA: Sage Publications.

Levy, S. 1984. *Hacker: Heroes of the Computer Revolution*, New York: Bantam Doubleday Dell.

Li, X. 1992. Lun Jusuanji Fanzui Xingfa Shiyong Wenti (Concerning the Application of Penal Law to Computer Crime), Graduate Law Review, *China University of Political Science and Law*, number 2.

Li, X. 1993. Jisuanji Fanzui Ruogan Wenti zhi Yanjiu (*A Study on Several Issues of Computer Crime)*, degree thesis for Master of Laws, China University of Political Science and Law.

Li, X. 2003. Lun Wangluo Fanzui (Crimes on the Internet), *Law Library*. Retrieved 15 February 2016, from http://www.law-lib.net/lw

Li, X. 2005a. Spam solutions: a law and economics view. International conference on law and economics and related topics, Helsinki, Finland.

Li, X. 2005b. Economic analysis of cybercrime: the mixed provision of private goods. In: Roufagalas, John (Ed.). Resource Allocation and Institutions: Explorations in Economics, Finance and Law (607−620). Athens, Greece: ATINER.

Li, X. 2006a. Cybersecurity as a Relative Concept. *Information & Security: An International Journal*, 18, pp. 11−24.

Li, X. 2006b. E-marketing, Unsolicited Commercial E-mail, and Legal Solutions. *Webology*, 3 (1), pp. 1−15.

Li, X. 2007a. International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene. *Webology*, 4 (3), pp. 1−15.

Li, X. 2007b. The Phenomenon of Unsolicited E-mails with Attachments. *SIMILE: Studies In Media & Information Literacy Education*, 7 (2), pp. 1−11.

Li, X. 2008a. The Criminal Phenomenon on the Internet: Hallmarks of Criminals and Victims Revisited Through Typical Cases Prosecuted (2008). University of Ottawa Law & Technology Journal, Vol. 5, Nos. 1-2.

Li, X. 2008b. *Cybercrime and Deterrence: Networking Legal Systems in the Networked Information Society*, Turku: Uniprint.

Li, X. 2014a. Phenomenal exploration into impact of anonymity on law

and order in cyberspace. *Criminology & Social Integration Journal (Kriminologija i socijalna integracija)*, 22 (2), pp. 102–123.

Li, X. 2014b. Exploring into regulatory mode for social order in cyberspace. *Webology*, 11 (2), 1–8.

Li, X. 2015. Cyberspace and the Informed Rationality of Law. *The Romanian Journal of Sociology*, 26, pp. 3–27.

Lilley, P. 2002. *Hacked, Attacked, and Abused: Digital Crime Exposed*, London, U. K.: Kogan Page Limited.

Lilley, P. 2003. *Dirty Dealing: The World Truth about Global Money Laundering*, International Crime and Terrorism, second edition, London: Kogan Page Limited.

Linklater, A. 2000. *International Relation: Critical Concepts in Political Science*, London: Routledge.

Loeb, M. P. 1 April 2004. The True Cost of Cybercrime, *Network Computing*.

London School of Economics and Political Science. 2001. Cybercrime: the Challenge to Leviathan? Retrieved 15 February 2016, from http://www.lse.ac.uk/clubs/hayek/Essays/cybercrime.htm

Longstaff, T. A. 1999. International Coordination for Cyber Crime and Terrorism in the 21st Century, presentation at *the Conference on International Cooperation to Combat Cyber Crime and Terrorism*, Hoover Institution, Stanford University, Stanford, California, 6-7 December.

Longstaff, T. A. and co-workers. 1997. Security of the Internet, in *The Froehlich/Kent Encyclopedia of Telecommunications*, New York: Marcel Dekker, volume 15, 231-255.

Macedo, S. 2004. *Universal Jurisdiction: National Courts and the Prosecution of*

Serious Crimes Under International Law, Philadelphia, Pennsylvania: University of Pennsylvania Press.

Mackenizie, E., and Goldman, K. 2000. Computer Abuse, Information Technologies and Judicial Affairs, in *Proceedings of the 28th Annual ACM SIGUCCS Conference on User Services: Building the Future*, pp. 170-176.

MacKinnon, R. C. 1997. Punishing the Persona: Correctional Strategies for the Virtual Offender, in S. G. Jones. (ed.). *Virtual Culture: Identity and Communication in Cybersociety*, London: SAGE Publications, pp. 206-235.

Maiwald, E. 2003. *Network Security: A Beginner's Guide*, second edition, California: McGraw-Hill Osborne Media.

Mandia, K. and Prosise, C. 2003. *Incident Response and Computer Forensics*, Emeryville, California: McGraw-Hill/Osborne.

Rosenberg. M. J. 2001. *E-Learning: Strategies for Delivering Knowledge in the Digital Age*, McGraw-Hill.

Marshall, E. 1988. The Worm's Aftermath: Computer experts meeting at Fort Meade decide there are no hidden threats to Internet; officials weigh criminal charges against a brilliant hacker, Science, 25 November, vol. 242. no. 4882, pp. 1121 - 1122, DOI: 10.1126/science.242.4882.1121.

Maslow, A. H. 1954. *Motivation and Personality*, New York: Harper.

McAfee. 2005. *Virtual Criminology Report: North American Study into Organized Crime and the Internet*.

McAfee. 2013. The Economic Impact of Cybercrime and Cyber Espionage.

McConnell International. 2000. Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information. Retrieved 15 February 2016, from http://www.witsa.org/papers/McConnell-cybercrime.pdf.

McCullagh, D. 19 August 2004. Punishment Fails to Fit the Cybercrime, *ZDNet United Kingdom*. Retrieved 15 February 2016, from http://www.crime-research.org/news/19.08.2004/574/

McKenna, B. 2003a. United Kingdom Police Promise Charter to Guard Good Names, *Computers and Security*, volume 22, number 1, pp. 38-40.

McKenna, R. 2003b. *The Dictionary of Nautical Literacy*, Blacklick, OH: McGraw-Hill Companies.

McNamara, J. 2003. *Secrets of Computer Espionage: Tactics and Countermeasures*, John Wiley and Sons.

Meinel, C. 2004. Computer Hacking--Where Did It Begin and How Did It Grow? *Guide to Harmless Hacking, Beginners' Series*, number 5.

Menthe, D. 1998. Jurisdiction in Cyberspace: A Theory of International Spaces, *Michigan Telecommunications Law Review,* volume 4, pp. 69-103.

Mermin, S. 1973. *Law and the Legal System -- An Introduction*, Toronto: Little, Brown and Company.

Miethe, T. D. 1995. Fear and Withdrawal from Urban Life, in Wesley G. Skogan, ed. *Reactions to Crime and Violence*, Thousand Oaks, London, New Delhi: SAGE Periodicals Press, pp. 14-27.

Miettinen, J. E. 1996. *Survey of Hacking in Finland in the 1990s- Summary of the Results*, Oulu: University of Oulu.

Milhorn, H. T. 2005. *Crime: Computer Viruses to Twin Towers*, Boca Raton, Florida: Universal Publishers.

Ministry of Justice. 1985. *Proceedings of Seminar on Problems of Computer Crime*, Taipei: Communication of Justice Press.

Mitchell, C. 2012. The Cyber Crime Threat on Mobile Devices. Retrieved

15 February 2016, from chrismitchell.net/Papers/tcctom.pdf

Mitchell, S. D., and Banker, E. A. 1998. Private Intrusion Response, *Harvard Journal of Law and Technology*, volume 11, number 3, pp. 699-732.

Mohay, G., Byron, C., Vel, O., McKemmish R., and Anderson, A. 2003. *Computer and Intrusion Forensics*, Norwood, Massachusetts: Artech House.

Molnar, J. 1987. Putting Computer-related Crime in Perspective, *Journal of Policy Analysis and Management,* volume 6, number 4, Privatization: Theory and Practice, pp. 714-716.

Mosco, V. 2004. *The Digital Sublime: Myth, Power, and Cyberspace*, The MIT Press.

Mowrer, E. R. 1942. *Disorganization: Personal and Social*, Chicago, Philadelphia, New York: J. B. Lippinatt Company.

National Counterterrorism Centre. 2005. *A Chronology of Significant International Terrorism for 2004*.

Negroponte, N. 1995. A Bill of Writes, *Wired 3.05*.

Nelson, B. 1991. Straining the Capacity of the Law: The Idea of Computer Crime in the Age of the Computer Worm, *Computer Law Journal*, volume 11, number 2, pp. 299-321.

Nelson, M. 10 January 2004. Internet Security Systems' Chris Klaus Says Companies Should Close Back Doors to Be Secure, *InfoWorld*.

Nordic Council of Ministers. 2005. *Nordic Information Society Statistics 2005,* TemaNord 2005:562. Copenhagen: Nordic Council of Ministers.

Norges Offisielle Statistikk. 2007. Kriminalstatistikk 2002 (Crime Statistics 2002). Oslo: Statistik Sentralbyrå.

Nycum, S. H. 1983. Testimony on Computer Security before the U. S.

Senate Subcommittee on Oversight of Government Management of the Committee on Governmental Affairs, *Computers and Society*, volume 13, number 4 and volume 14, Nos. 1, 2, and 3.

Oberding, J. M. and Norderhaug, T. 1996. A Separate Jurisdiction for Cyberspace? *Journal of Computer-Mediated Communication,* volume 2, number 1. Retrieved 15 February 2016, from http://jcmc.indiana.edu/vol2/issue1/juris.html

O'Brien, T. 12 November 2004. Risk and Conflict Challenges for New Zealand, *Auckland War Memorial Museum Symposium Push for Peace*.

OECD. 2002. *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*.

Okin, J. R. 2004. *The Internet Revolution: The Not-for-dummies Guide to the History, Technology, and Use of the Internet*, Winter Harbor: Ironbound Press.

Overill, R. E. 1998. Computer crime - An Historical Survey. Retrieved 15 February 2016, from http://www.kcl.ac.uk/orgs/icsa/Old/crime.html.

Palczewski, C. H. 2001. Cyber-Movements, New Social Movements, and Counterpublics, in D. Brouwer and R. Asen. (eds.). *Counterpublics and the State*, New York: SUNY Press, 2001, pp. 161-186.

Parker, D. B. 1976. *Crime by Computer*, Charles Scribner's Sons, New York.

Parker, D. B. 1980. Computer Abuse Research Update, *Computer/Law Journal*, vol. II, no. 2, pp. 329-352.

Parker, D. B. 1989. *Computer Crime: Criminal Justice Resources Manual*, National Institute of Justice.

Parker, D. B. 1998. *Fighting Computer Crime: A New Framework for Protecting Information*, New York, N.Y.: John Wiley and Sons.

Parker, D. B., and Nycum, S. H. 1984. Computer Crime, *Communication of the ACM*, volume 27, number 4, pp. 313-315.

Parker, R. 1990. Computer-Related Crime: Ethical Considerations: (With Application for Teaching Computer Literacy Classes), *Computers and Society*, volume 20, number 3, pp. 180-191.

Perle, E. G. and co-workers. 2000. Electronic Publishing and Software, Part 1, *Computer Law*.

Perrin, S. 2005. Cybercrime, in Alain Ambrosi, Valerie Peugeot and Daniel Pimienta. (eds.). *Word Matters: Multicultural Perspectives on Information Societies*, C and F Editions. Retrieved 15 February 2016, from http://www.vecam.org/article658.html

Peters, A. 1971. *Computers and Society: A Course*, IIT, pp. 30-38.

Peterson, T. F. 2003. *Nightwork: A History of Hackers and Pranks at MIT*, Massachusetts: Massachusetts Institute of Technology Press.

Pethia, R. D. 2001. Information Technology—Essential But Vulnerable: How Prepared Are We for Attacks? Before the House Committee on Government Reform,

Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, 26 September. Retrieved 15 February 2016, from http://www.cert.org/congressional_testimony/Pethia_testimony_Sep26.html

Pew Research Center. (2015). Social Networking Fact Sheet. Retrieved 15 February 2016, from http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/

Philip, A. R. 2002. *The Legal System and Ethics in Information Security*, SANS Institute. Retrieved 15 February 2016, from http://www.securitydocs.com/go/1604

Pickett, J. P. and co-workers. 2000. The American Heritage Dictionary of the English Language, fourth edition, Boston: Houghton Mifflin Company.

Pihlajamäki, A. 2004. *Tietojenkäsittelyrauhan rikosoikeudellinen suoja: datarikoksia koskeva sääntely Suomen rikoslaissa* (The Protection of Data Processing under Criminal Law: Provisions on Data Crimes in the Finnish Criminal Code), Helsinki: Suomalainen lakimiesyhdistys.

Pipkin, D. L. 2002. *Halting the Hacker: A Practical Guide to Computer Security (with CD-ROM)*, Englewood Cliffs, New Jersey: Prentice Hall PTR.

Police Commissioners' Conference Electronic Crime Working Party. 2000. *The Virtual Horizon: Meeting the Law Enforcement Challenges: Developing an Australasian Law Enforcement Strategy for Dealing With Electronic Crime*. Scoping Paper, Adelaide: Australasian Centre for Policing Research, Report Series No: 134.1.

Pollitt, M. A. 1997. Cyberterrorism: Fact or Fancy? *Proceedings of the 20th National Information Systems Security Conference*. Cited in K. Hudnall Robert, *No Safe Haven: Homeland Insecurity*, El Paso, Texas: Omega Press, 2004, p. 124.

Post, D. G. 1996. Governing Cyberspace, *Wayne Law Review*, volume 43, pp. 155-171.

Preston, E., and Lofton, J. 2002. Computer Security Publications: Information Economics, Shifting Liability and its First Amendment, *Whither Law Review*, volume 24.

Putnam, T. L, and Elliott, D.D. 2001. International Responses to Cyber Crime, in Abraham D.

PwC. 2015. US Cybersecurity: Progress Stalled, Key Findings from the 2015 US State of Cybercrime Survey. Delaware, US: PricewaterhouseCoopers.

Sofaer, A. D., and Seymour E. G. (eds.). *The Transnational Dimension of Cyber Crime and Terrorism*, Hoover Institution, 2001, pp. 35-68.

Radzinowicz, L. and King, J. 1977. *The Growth of Crime: The International Experience,* London: Hamish Hamilton.

Randall, K. N., Ryan, D. J., and Ryan, J. 2000. *Defending Your Digital Assets Against Hackers, Crackers, Spies, and Thieves*, McGraw-Hill.

Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D. and Moore, A. 2004. *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*, Carnegie Mellon Software Engineering Institute.

Raymond, E. S. 2001. *The Cathedral and the Bazaar*, Sebastopol, California: O'Reilly and Associates.

Reece, D. 3 December 2000. The Hacker Cracker, *The Sunday Telegraph*, volume 14.

Rees, A. 2000. *ACPR Technology Environment Scan*, Report number 133.1, Adelaide: Australasian Centre for Policing Research.

Shoni, R., Jackson, P., Hollmen, L. and Aspnäs, M. (eds.). 1998. *Teleworking Environment: Proceedings of the Third International Workshop on Telework*, Turku, Finland, 1-4 September 1998. Turku Centre for Computer Science.

Rosenblatt, K. 1990. Deterring Computer Crime, *Technology Review*, volume 93, number 2, pp. 34-40.

Roush, W. 1995. Hackers: Taking a Bite Out of Computer Crime, *Technology Review*.

Rowland, D. 1998. Cyberspace - A Contemporary Utopia? *The Journal of Information, Law and Technology*, volume 1998, number 3. Retrieved 15 February 2016, from http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1998_3/rowland/

Reynolds, G. 2003. *Ethics in Information Technology*, Thomson Course Technology.

RSA. 2015. Cybercrime 2015: An Inside Look at the Changing Threat Landscape. Retrieved 15 February 2016, from http://www.emc.com/collateral/white-paper/rsa-white-paper-cybercrime-trends-2015.pdf

Sadowsky, G., Dempsey, J. X., Greenberg, A., Mack, B.J., and Schwartz, A. 2003. *Information Technology Security Handbook*, Washington, DC: The International Bank for Reconstruction and Development.

Salgado, R. P. 2001. Working with Victims of Computer Network Hacks, *USA Bulletin*, volume 49, number 2.

Samuelson, P. 1989. Can Hackers Be Sued for Damages Caused by Computer Viruses? *Communications of the ACM*, volume 32, number 6, pp. 661-669.

Schjolberg, S., and Hubbard, A. M. 2005. Harmonizing National Legal Approaches in Cybercrime, 10 June 2005, International Telecommunication Union, *WSIS Thematic Meeting on Cybersecurity*, Geneva, 28 June-1 July.

Schjolberg, S. 2004. Computer-Related Offences, A Presentation at *the Octopus Interface 2002- Conference on the Challenge of Cybercrime,* 15-17

September, Council of Europe, Strasbourg, France. Retrieved 15 February 2016, from http://cybercrimelaw.net/documents/Strasbourg.pdf

Schneier, B. 2004. Hacking the Business Climate for Network Security, *Computer*, volume 37, number 4, pp. 87-89.

Schwartau, W. 1994. *Information Warfare: Chaos on the Electronic Superhighway*, New York: Thunder's Mouth Press.

Schweinhart, L. J., Barnes, H. V., and Weikart, D. D. 1993. *Significant Benefits: The High/Scope Perry Preschool Study Through Age 27*, Ypsilanti, MJ: High/Scope Press.

Science Applications International Corporation (SAIC). 1997. *Organization and Business Case Model for Information Security*.

Selwyn, N., and Gorard, S. 2001. *101 Key Ideas in Information Technology*, United Kingdom, United States of America: Hodder and Stoughton-McGraw-Hill.

Shannon, L. R. 21 March 1993. The Happy Hacker, *New York Times*, p. 2.

Shaw, E. D., Ruby, K. G., and Post, J. M. 1998. The Insider Threat to Information system, *Security Awareness Bulletin*, number 2-98. Retrieved 13 March 2007, from http://rf-web.tamu.edu/security/secguide/Treason/Infosys.htm.

Sherman, L. W. 1995. Public regulation of Private Crime Prevention, in Wesley G. Skogan. (ed.). *Reactions to Crime and Violence*, Thousand Oaks, London, New Delhi: SAGE Periodicals Press, pp. 102-113.

Sieber, U. 1996. *Computer Crime and Criminal Information Law - New Trends in the International Risk and Information Society* - Statement for the Hearing on Security in Cyberspace of the United States Senate, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, 16

July.

Sieber, U. 1998. *Legal Aspects of Computer-Related Crime in the Information Society, The COMCRIME-Study for the European Commission*. Retrieved 15 February 2016, from http://ec.europa.eu/archives/ISPO/legal/en/comcrime/sieber.html

Sinrod, E. J., and Reilly, W. P. 2000. Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws, *Computer and High Technology Law Journal*, volume 16, pp. 177-232.

Sjögren, H., and Skogh, G. 2004. Introduction, In Hans Sjögren and Göran Skogh eds. *New Perspectives on Economic Crime*, Edward Elgar Publishing, pp. 1-4.

Smith, B. D. 1998. *Psychology: Science and Understanding*, McGraw-Hill.

Smith, G. 8 September 1998. Truth is the First Casualty of Cyberwar, *Wall Street Journal.*

Smith, R. G., Grabosky, P. and Urbas, G. 2004. *Cyber Criminals on Trial*, Cambridge: The Press Syndicate of the University of Cambridge.

Smolen, M., and Downing, R. W. 2002. *Legal Framework for Combating Cybercrime, Components of Substantive Network Crimes Laws: How to Criminalize Attacks on Computer Networks and Information*, 17-18 August.

Sofaer, A. D. and co-workers. 2000. *A Proposal for an International Convention on Cyber Crime and Terrorism*, Centre for International Security and Cooperation.

Sofaer, A. D. and Goodman, S. E. 2005. *The Transnational Dimension of Cyber Crime and Terrorism*, Hoover Press.

Solarz, A. 1981. *Computer Technology and Computer Crime*, Stockholm, Sweden:

Research and Development Division.

Speer, D. L. 2000. Redefining Borders: The Challenges of Cybercrime, *Crime, Law and Social Change*, volume 34, pp. 259-273.

Stanley, T. J. 1995. Optimal Penalties for Concealment of Crime, *Economics Working Paper Archive*.

Statista. 2015. Types of cyber crime in companies in Germany 2015. Retrieved 14.10.2015, from http://www.statista.com/statistics/429635/cyber-crime-in-companies-germany/

Statistics Denmark. 2006. Statistics Yearbook 2006. Copenhagen: Statistics Denmark.

Stephenson, P. 2000. *Investigating Computer-Related Crime*, Boca Raton: Florida: CRC Press LLC.

Sterling, B. 1994. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, Austin, Texas: Electronic Release. Retrieved 15 February 2016, from http://www.gutenberg.org/dirs/etext94/hack12.txt

Stoll, C. 1988. Stalking the Wily Hacker, *Communication of the ACM*, volume 31, number 5, 484-497. Reprinted in C. Dunlop and R. Kling (eds.) *Computerization and Controversy: Value Conflicts and Social Choices*, San Diego: Academic Press, 1991, pp. 524-532.

Summers, D. (director). 2003. *Longman Dictionary of Contemporary English*, Essex, England: Pearson Education Limited.

Sutherland, E. H. 1949. *White Collar Crime,* New York: Holt, Rinehart and Winston.

Sutherland, E. H. 1983. *White Collar* Crime (the uncut version), with an

introduction by Gilbert Geis and Colin Goff, New Haven and London: Yale University Press.

Syngress. 2002. *Scene of the Cybercrime: Computer Forensics Handbook*, Rockland, MA: Syngress Publishing.

Tapscott, D. 1996. *The Digital Economy: Promise and Peril in The Age of Networked Intelligence*, McGraw-Hill.

Tavani, H. T. 2000. Defining the Boundaries of Computer Crime: Piracy, Break-ins, and Sabotage in Cyberspace, *Computers and Society*, volume 30, number 4, pp. 3-9.

Taylor, M. and Quayle, E. 2003. *Child Pornography: An Internet Crime*, East Sussex: Brunner-Routledge.

Technical Working Group for Electronic Crime Scene Investigation. 2001. *Electronic Crime Scene Investigation: A Guide for First Responders*, National Institute of Justice, Office of Justice Program, the United States Department of Justice.

Telang, R, and Wattel, S. 2005. Impact of Vulnerability Disclosure on Market Value of Software Vendors: An Empirical Analysis, Presented at *the Fourth Workshop on Economics and Information Security, Boston*, 1-3 June.

Tennyenhuis, A. and Jamieson, R. 2003. Multidisciplinary E-Forensics Methodology Development to Assist in the Investigation of E-Crime, in Kim Viborg Anderson, Steve Elliot, and Paula M. C. Swatman, eds. *Seeking Success in E-Business: A Multidisciplinary Approach*, Norwell, Massachusetts: Kluwer Academic Publishers, 2003, pp. 187-206.

The Article 29 Data Protection Working Party. 2001. Fourth Annual Report on the Situation Regarding the Protection of Individuals with

regard to the Processing of Personal Data and Privacy in the Community and in the Third Countries Covering the Year 1999.

The Mentor. 8 January 1986. The Conscience of a Hacker (known as "The Hacker's Manifesto" or "The Hacker Manifesto"). *Phrack*, volume 1, issue 7, Phile 3 of 10. Retrieved 15 February 2016, from http://www.phrack.org/issues.html?issue=7&id=3#article

Thomas, D. 2002. *Hacker Culture*, Minneapolis, Minnesota: The University of Minnesota Press.

Thomas, W. I. and Znaniecki, F. 1927. *The Polish Peasant in Europe and America*, New York: Alfred E. Knopf.

Thompson, D. 1989. Police Powers - Where's the Evidence? *Proceedings of The Australian Computer Abuse Inaugural Conference*.

Tullock, G. 1967. The Welfare Costs of Tariffs, Monopolies and Theft, *Western Economic Journal*, volume 5, pp. 224-232.

UN. 2000. Crimes Related to Computer Networks: Background Paper for *the Workshop on Crimes Related to the Computer network, Tenth UN Congress on the Prevention of Crime and the Treatment of Offenders,* Vienna, 10-17 April. A/CONF. 187/10.

UNCJIN. 1999. International Review of Criminal Policy -United Nations Manual on the Prevention and Control of Computer-Related Crime, *International Review of Criminal Policy*, nos. 43 and 44.

United Nations Economic Commission for Africa. 2014. Tackling the challenges of cybersecurity in Africa. Retrieved 15 February 2016, from www.uneca.org/sites/default/files/.../ntis_policy_brief_1.pdf

UNODC. 2013. Comprehensive Study on Cybercrime. Vienna: United

Nations Office on Drugs and Crime.

U. S. Congress, Office of Technology Assessment, September 1989. *Polar Prospects: A Minerals Treaty for Antarctica*. OTA-O-428, Washington, DC: U. S. Government Printing Office.

U. S. Department of Justice. 17 May 2002. Warez Leader Sentenced to 46 Months, *Press Release*.

U. S. Department of Justice. 2000. *The Electronic Frontier: the Challenge of Unlawful Conduct Involving the Use of the Internet-- A Report of the President's Working Group on Unlawful Conduct on the Internet*.

U. S. Department of Justice. 2003. Frequently Asked Questions and Answers-Council of Europe Convention on Cybercrime. Retrieved 15 February 2016, from http://www.cybercrime.gov/COEFAQs.htm

U. S. Department of Justice. 24 September 2001. B. K. West, Employee of Oklahoma ISP, Pleads Guilty to Unauthorized Access Charge Under 18 U.S.C. S 1030(a)(2)(c), *Press Release*.

U. S. Government, 2006. *Budget of the United States Government Fiscal Year 2006*, US Government Printing Office, Washington.

Vacca, J. R. 2005. *Computer Forensic: Computer Crime Scene Investigation*, Hingham, Massachusetts: Charles River Media.

Vamosi, R. 10 September 2003. Make the Punishment Fit the Cybercrime, *CNET Reviews*. Retrieved 15 February 2016, from http://reviews.cnet.com/4520-3513_7-5073597-1.html

Van Dervort, T. R. 1998. *International Law and Organization: An Introduction*, Thousand Oaks, California: Sage Publications.

Van Traa-Engelman, H. L. 1993. *Commercial Utilization of Outer Space: Law*

and Practice, Dordrecht, The Netherlands: Martinus Nijhoff Publishers.

Vatis, M. A. 1999. Congressional Statement, FBI, National Infrastructure Protection Centre (NIPC) Cyber Threat Assessment, Before the Subcommittee on Technology and Terrorism of the Senate Committee on the Judiciary, 6 October. Retrieved 15 February 2016, from http://www.fas.org/irp///congress/1999_hr/nipc10-6.htm

Vatis, M. A. 2000. *Senate Joint Cyberattack Investigation: Capitol Hill Hearing Testimony*, 106th Congress.

Vernant, J. (ed.). 1995. *The Greeks*, University of Chicago Press.

Walsh, D. P. 1983. Visibility, in Dermot Walsh and Adrian Poole (eds), *A Dictionary of Criminology*, London, Boston, Melbourne and Henley: Routledge and Kegan Paul.

Ware, H. W., Pfleeger, C. P. and Pfleeger, S. L. 2002. *Security in Computing, Englewood Cliffs*, New Jersey: Prentice Hall PTR.

Wasik, M. 1991. *Crime and the Computer*, Oxford: Clarendon Press.

Weimann, G. 2004. Cyberterrorism: How Real is the Threat? *United States Institute of Peace Special Report*, number 119.

Wells, T. D. and Sevilla, C. 2003. *Maximizing the Enterprise Information Assets*, Florida: Auerbach.

Westby, J. ed. 2003. *International Guide to Combating Cybercrime*, American Bar Association.

Williams, P. 13 August 2001. *Organized Crime and Cybercrime: Synergies, Trends, and Responses*, The Office of International Information Programs, the United States Department of State. Retrieved 15 February 2016, from http://usinfo.state.gov/journals/itgic/0801/ijge/gj07.htm

Wober, K. W., Frew, A. J. and Hitz, M. (eds.) 2002. *Information and Communication Technologies in Tourism 2002*, Wien: Springer Verlag.

Wood, M. B. 1982. *Introducing Computer Security*, The U.S.: NCC Publications.

World Summit on the Information Society (WSIS). 2003. Declaration of Principles. Building the Information Society: A Global Challenge in the New Millennium. Document WSIS-03/GENEVA/DOC/4-E. Geneva, 12 December 2003.

Yan, W. and Zhang, Y. 6 November 2001. Xinjiang's First Cybercrime 17-Year-Old Hacker Arrested, *Beijing Youth Daily*.

Yeager, Peter and Clinard, Mashall. 2006. *Corporate Crime*, Transaction Publishers.

Yi, M. 27 January 2006. Associated with Traditional Crime, Cybercrime Threats Citizens Safety, *Huanghai Morning Newspaper*.

Zeviar-Geese, G. 1998. The State of the Law on Cyberjurisdiction and Cybercrime on the Internet, *Gonzaga Journal of International Law*, volume 1.

Zhang, Z. 1999. *Introduction to International Law*, China University of Political Science and Law Press.

Zhao, Y. 1994. *Guoji Xingfa yu Sifa Xiezhu* (International Criminal Law and Justice Assistance), Beijing: Law Press.

Zheng, H. 2004. A Study on Cybercriminals, *Social Sciences Front*, number 6.

Toronto Academe Press

ISBN 978-0-9739813-3-9

9 780973 981339 >